PC actual
Guías prácticas
PISTAS & TRUCOS
SUPLEMENTO PC ACTUAL 204 + DVD ACTUAL

Máxima seguridad al utilizar tu PC

Backup

- Cómo hacer copias de seguridad
- Utiliza Cobian Backup 8

Privacidad

- Protege los datos de tu PC
- Blinda tus documentos en Windows Vista
- Aprovecha PGP Desktop



Equipos

- Convierte el PC en una caja fuerte
- Escaparate de productos

Internet

- Defiéndete de amenazas on-line
- Configura el cortafuegos
- Seguridad NAT con un router

Confidencialidad

- Navega de forma anónima
- Encripta mensajes con PGP

- Hardware y software para proteger tu equipo
- Accede con tranquilidad a redes wireless

Pagina Publicidad

guía práctica seguridad

Backup

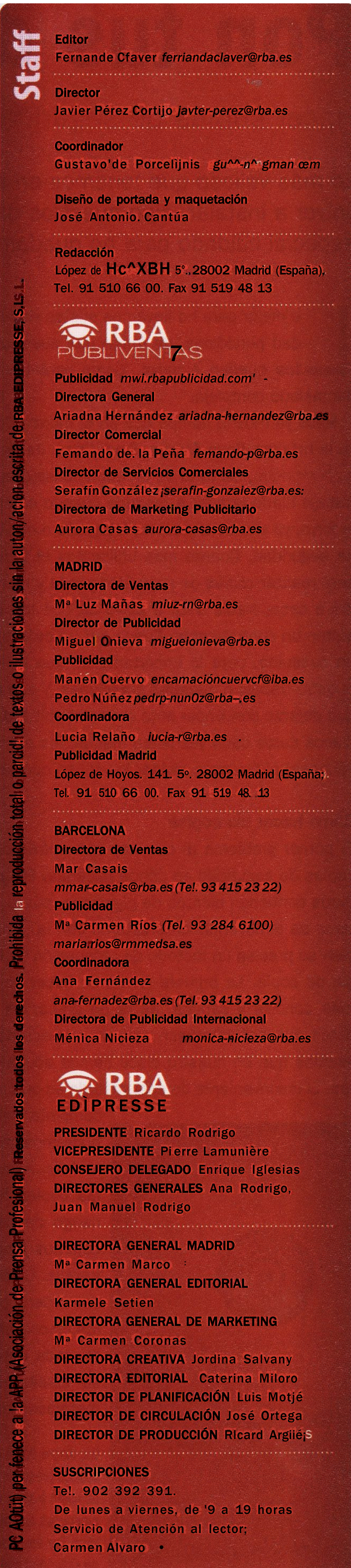
Privacidad

Equipos

Internet

Confidencialidad

Wireless



Staff

Editor
Fernande Cfaver *ferriandaclaver@rba.es*

Director
Javier Pérez Cortijo *javter-perez@rba.es*

Coordinador
Gustavo'de Porcelijnis *gu^^-n^gman œm*

Diseño de portada y maquetación
José Antonio. Cantúa

Redacción
López de Hc^XBH 5°..28002 Madrid (España).
Tel. 91 510 66 00. Fax 91 519 48 13

RBA PUBLIVENTAS

Publicidad *mwi.rbapublicidad.com'* -
Directora General
Ariadna Hernández *ariadna-hernandez@rba.es*
Director Comercial
Femando de. la Peña *femando-p@rba.es*
Director de Servicios Comerciales
Serafín González *¡serafin-gonzaiez@rba.es:*
Directora de Marketing Publicitario
Aurora Casas *aurora-casas@rba.es*

MADRID
Directora de Ventas
Mª Luz Mañas *miuz-rn@rba.es*
Director de Publicidad
Miguel Onieva *migueionieva@rba.es*
Publicidad
Manen Cuervo *encamacióncuervcf@iba.es*
Pedro Núñez *pedrp-nun0z@rba–.es*
Coordinadora
Lucia Relaño *iucia-r@rba.es*
Publicidad Madrid
López de Hoyos. 141. 5º. 28002 Madrid (España).
Tel. 91 510 66 00. Fax 91 519 48. 13

BARCELONA
Directora de Ventas
Mar Casais
mmar-casais@rba.es (Te!. 93 415 23 22)
Publicidad
Mª Carmen Ríos *(Tel. 93 284 6100)*
maria.rios@rmmedsa.es
Coordinadora
Ana Fernández
ana-fernadez@rba.es (Tel. 93 415 23 22)
Directora de Publicidad Internacional
Ménica Nicieza *monica-nicieza@rba.es*

RBA EDIPRESSE

PRESIDENTE Ricardo Rodrigo
VICEPRESIDENTE Pierre Lamunière
CONSEJERO DELEGADO Enrique Iglesias
DIRECTORES GENERALES Ana Rodrigo, Juan Manuel Rodrigo

DIRECTORA GENERAL MADRID
Mª Carmen Marco
DIRECTORA GENERAL EDITORIAL
Karmele Setien
DIRECTORA GENERAL DE MARKETING
Mª Carmen Coronas
DIRECTORA CREATIVA Jordina Salvany
DIRECTORA EDITORIAL Caterina Miloro
DIRECTOR DE PLANIFICACIÓN Luis Motjé
DIRECTOR DE CIRCULACIÓN José Ortega
DIRECTOR DE PRODUCCIÓN Ricard Argiiés

SUSCRIPCIONES
Te!. 902 392 391.
De lunes a viernes, de '9 a 19 horas
Servicio de Atención al lector;
Carmen Alvaro

Pon tus datos a salvo

Hacer copias de seguridad nos ahorrará algún que otro disgusto

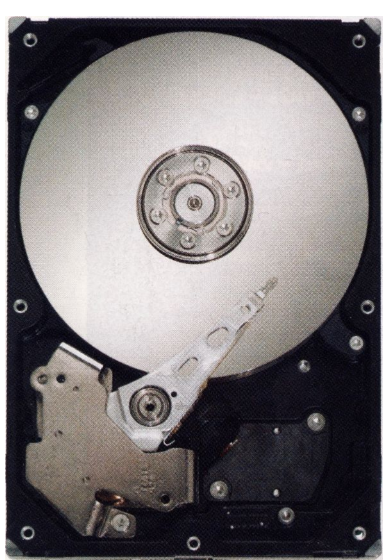
Lo más valioso que tenemos en el PC no son los programas, que al fin y al cabo siempre podremos volver a instalar, sino nuestros datos. Nuestros documentos son insustituibles y hemos de tener especial cuidado para no quedarnos sin ellos por un problema del disco duro o por borrarlos por error.

Lo mejor para no llevarnos sustos es realizar copias de seguridad periódicas, de forma que nuestros datos más importantes queden a salvo. Como veremos, no es una operación demasiado compleja.

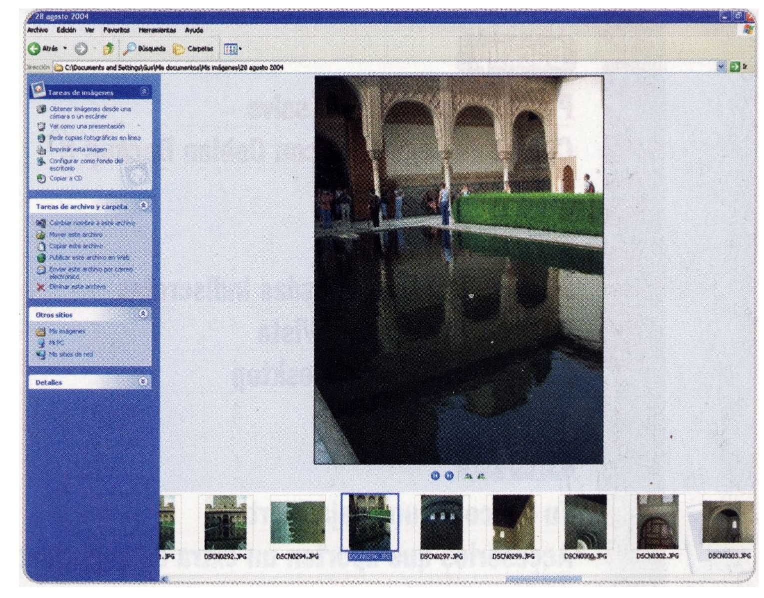
Hace ya mucho tiempo que en el mundo de la informática se utiliza la máxima *Save Always, Save Oñen,* es decir, graba siempre, graba a menudo. Se trata de un buen consejo aplicable tanto a nuestro trabajo diario (grabar a menudo cuando estemos trabajando con un archivo, ya sea de texto, una fotografía o un vídeo) como a las copias de seguridad. Cuanto más utilicemos el ordenador, más necesario será realizar copias de seguridad y más a menudo deberíamos llevarlas a cabo. Nadie está a salvo de que los datos de su ordenador sufran un contratiempo. Puede ser un defecto del sistema, un virus, un descuido, pero lo importante es que la víctima de todo eso es nuestro trabajo o nuestras creaciones, y eso es insustituible. No hay que dejarse convencer ante la improbabilidad de que algo ocurra (los discos duros cada vez fallan menos, los antivirus son cada vez más eficaces) ni tampoco olvidar lo valioso que son nuestros datos.

Cómo hacer las copias

El primer problema al que hay que enfrentarse a la hora de hacer copias de seguridad es dónde hacerlas. En la actualidad, los discos duros contienen cientos de gigabytes, por lo que se requiere yn sistema de almacenamiento externo con la suficiente capacidad. También se precisa un método de ordenación de los datos y una estrategia de copia. La primera forma de hacer copias de seguridad, y la más sencilla y caótica, es la de grabar en soportes externos los datos que nos interesan cuando nos acordemos de ello o cuando veamos que en nuestro disco hemos acumulado ficheros importantes. El inconveniente de este método es que no tendremos una copia completa del disco, con lo que no podremos recuperar el sistema de un fallo. Además, si la frecuencia de las copias no es fija, corremos el riesgo de perder muchos datos si dejamos mucho tiempo entre copia y copia. Un problema adicional es el del orden, pues hemos de revisar los discos para saber qué cosa hay en cada uno de ellos. En realidad, se suelen escoger procesos más metódicos para las copias de seguridad y que están implementados en los programas de *backup,* que facilitarán enormemente la tarea de mantener nuestros datos a salvo. Además de la mencionada, existen múltiples métodos o estrategias para realizar las copias de seguridad.



Los discos duros que se fabrican actualmente pueden presumir de una fiabilidad mayor, pero no están a salvo de problemas y sobre todo de programas que destruyan sus datos, como los virus. Por eso, nunca está de más realizar copias de seguridad periódicas.

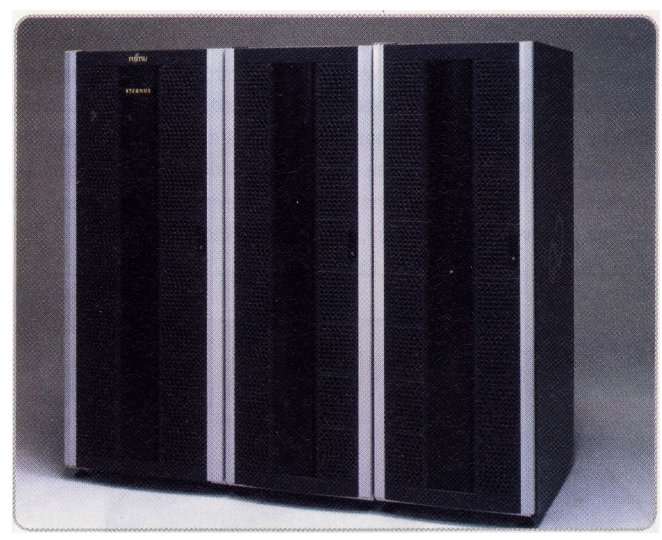


El primer acercamiento al ***backup*** es tener copias de los ficheros que más nos interesan a buen recaudo. En este caso, es mejor guardar los archivos con fotografías y documentos que los ficheros de los programas, ya que éstos podemos recuperarlos.

Diferentes sistemas

El primero y más seguro es la copia total, es decir, realizar y almacenar una imagen del disco duro que queremos proteger. Es un sistema que presenta un problema principal, y es el del almacenamiento, ya que tendremos que guardar copia de una gran cantidad de datos. Como complemento a este tipo de *backup* existen dos variantes, la incrementai y la diferencial. La primera parte de una copia total va almacenando solamente los datos que hayan variado. De esta forma, tendremos una copia de todos los datos sin tener que realizar una copia total periódicamente. Eso sí, para devolver el disco al último estado operativo tendremos que recuperar primero la copia total y luego todas las incrémentales, por lo que el proceso es largo.

La otra variante es la copia total y diferencial. Se distingue de la anterior en que, después de realizar la primera, se van copiando cada vez que se actualicen todos los ficheros que hayan cambiado, y no sólo los que hayan sido modificados con respecto a la copia anterior. Esto presenta el inconveniente de que se necesita mayor capacidad de almacenamiento, pero no es necesario recuperar todas las copias realizadas antes de la recuperación. Otro método de copia es el del espejo, más conocido por su traducción en inglés (*mirror).* Se trata de una réplica de nuestro disco duro. Se realiza una copia total inicial, como en los métodos anteriores, pero, a continuación,



Las copias de seguridad son importantes en un ordenador personal, pero se pueden considerar vitales en sistemas grandes, ya que tienen almacenados una gran cantidad de datos tan sensibles, por ejemplo, como los personales o financieros.

esa copia se ve modificada cada vez que hay cambios en nuestro disco duro. De esta forma, siempre tendremos a nuestra disposición una única copia de todos los datos del disco. Las totales o las que están sin estructurar se pueden realizar con medios de almacenamiento removibles, como DVD o CD. Sin embargo, las copias por *mirror*tienen que realizarse con un sistema de almacenamiento que pueda actualizarse a menudo, como un disco duro (externo o Interno) o un sistema de almacenamiento en red.

Uno de los últimos sistemas de copia de seguridad es el de continua, Jlamado CDP o *Continuous Data Protection.* Este tipo de sistemas almacena en un soporte todos los cambios en los discos objeto de la protección en cualquier momento. Es decir, que no existe una programación de coplas, sino que los discos duros están constantemente siendo copiados. No requiere tanto espacio como una copia diferencial o incluso ¡ncremental, ya que sólo se almacenan los cambios a nivel de bytes o bloques, mientras que las copias totales guardan los ficheros completos que han cambiado. La gran ventaja del CDP es que es posible recuperar el estado del disco en cualquier punto del tiempo, por lo que se reduce el peligro de perder información importante.

Selección y extracción

Además de los métodos de copia, estos sistemas necesitan un método a seguir para decidir qué datos tienen que copiar y de qué manera. Es posible copiar simplemente los ficheros importantes a través de las herramientas de copia del sistema operativo, pero lo más seguro es mantener una copia del disco que permita restaurar tanto los ficheros como el sistema operativo y los programas instalados en él para seguir utilizando el ordenador tras cualquier problema que pueda deteriorar el contenido del disco. Este tipo de sistemas requieren un software de *backup* específico, como puede verse en el recuadro correspondiente. Estos programas son capaces de hacer copias de seguridad de ficheros que están siendo utilizados, pero también guardan las características del sistema de archivos para que la recuperación sea completa.

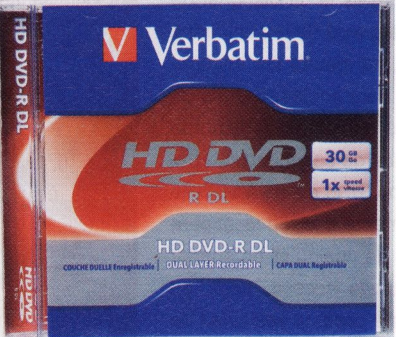


Aunque la relación capacidad-precio de los discos duros externos les hace una dura competencia, en el mercado se siguen encontrando sistemas de copla de seguridad basados en cinta magnética.

Seguridad con sistemas RAID

Es el acrónimo de *Redundant Array of Independent Disks*, es decir, bloque redundante de discos independientes. Se trata de un grupo de discos que se utilizan como soporte para almacenar datos de forma reduntante con distintas finalidades. Es decir, en vez de utilizar un solo disco se utilizan varios que almacenan los mismos datos. Estos sistemas son transparentes para el sistema operativo, es decir, que para el usuario aparecen como un único disco. Los usos de un sistema RAID son principalmente los siguientes. El *mirroringo* **copias espejo** consiste en copiar los mismos datos en más de un disco. Esto aumenta la seguridad de los datos, ya que se encuentran físicamente en más de un disco, y también la velocidad de lectura. Sin embargo, hace que la velocidad de escritura sea menor, al tener que almacenar un mismo grupo de datos en distintos discos. El *stripping* consiste en **dividir los elementos de un archivo en más de un disco.** Esto permite un aumento de las prestaciones. La corrección de errores ralentiza el sistema de lectura y escritura, pues varias copias de los mismos datos se comparan para detectar posibles problemas, pero permiten atajar e incluso prevenir posibles errores en el disco. El objetivo del RAID es aumentar las prestaciones de los discos y mejorar la seguridad de ios datos. Se utiliza en grandes sistemas, pero también puede instalarse en ordenadores personales de altas prestaciones. Para disponer de un RAID en nuestro PC, la controladora que incorpora ia placa base debe tenerlo implementado. En otro caso, tendremos que adquirir una controladora de discos que funcione con ese sistema.





La llegada de los nuevos discos de alta capacidad, tanto Blu-ray Disc como HD DVD, ofrece nuevas posibilidades para la realización de copias de seguridad. De momento, sin embargo, el precio del soporte y de las unidades no los hace competitivos.

Sistemas de almacenamiento

Como hemos visto, las copias de seguridad requieren una considerable capacidad de almacenamiento de datos. Para hacer frente a este punto pueden utilizarse distintos sistemas, desde los más comunes hasta soluciones específicas para estas tareas. En primer lugar, el soporte más utilizado, por ser el más económico, es el CD. Resulta útil si sólo vamos a hacer copia de algunos documentos importantes, como archivos de texto o fotos, pero no necesitamos guardar una imagen completa del disco duro. Es necesario almacenarlos con cuidado, pues si se rayan pueden sufrir daños y entonces la copia no serviría para nada. También pueden utilizarse para hacer copias tota-



Algunas placas base Incorporan en el controlador de discos el sistema RAID con el que podremos aumentar sus prestaciones e incrementar la seguridad de los datos. Hay que tener en cuenta que, en ese caso, necesitaremos más de un disco duro.

les, pero esto supone una gran cantidad de discos, con lo engorroso que resulta. Hay que recordar que, como máximo, los CD almacenan 700 megabytes. Los DVD grabables son una solución que permiten tanto las copias parciales como las totales, ya que con su capacidad de 4,7 Gigabytes (los discos de una sola capa) facilitan realizar copias completas con un número de discos mucho menor que si se tratara de CD. También hay que tener en cuenta que el precio por Megabyte suele ser más bajo en este caso. Tanto con los CD como con los DVD, podemos optar por discos regrabables, es decir, que pueden utilizarse más de una vez. En este caso, sin embargo, el coste del soporte es mucho mayor. También es posible encontrar en el mercado discos DVD-RAM, que también permiten múltiples grabaciones y borrados. Sin embargo, son costosos y se requiere una unidad de disco especial para utilizarlos. Con la llégada de los discos HD DVD y Blu-ray Disc, la capacidad para los discos ópticos se multiplica (hasta 54 Gigabytes en un disco Blu-ray de doble capa). Podrfan constituir un soporte ideal para cojóias de seguridad, pero el coste tanto de las unidades de disco pomo de los consumibles aún es demasiado alto. Eso sí, lo que invirtamos en estos sistemas lo sacaremos como beneficio en comodidad, pues una copia completa ocupará unos pocos discos.

Discos duros externos

Una opción que empieza a resultar interesante es la de disponer de un disco duro ext^múTGracias a la bajada de precio de las unidades ^del-desarrolío de la velocidad de conexión, no resulta tan engorroso y caro disponer de un disco externo sólo para copias. Incluso es posible tener una sola carcasa conectable al ordenador y distintos discos duros donde almacenaremos las copias de seguridad. Se trata del sistema más rápido si lo conectamos por USB o FireWire. También existen discos que se conectan directamente a la red local para hacer copias de cualquier ordenador que tenga acceso, pero, en este caso, la velocidad de copia estará limitada a la de la conexión (por cable o inalámbrica). Otra forma de utilizar los discos duros para salvaguardar los datos, en este caso nos referimos a unidades internas, son los sistemas RAID. En el recuadro del mismo nombre se puede ver cómo funciona este sistema. La versatilidad de estos discos nos permite llevarlos con nosotros y utilizar nuestros datos en cualquier otro ordenador. Por otro lado, gracias a su capacidad y prestaciones, podremos hacer copias sin necesidad de utilizar programas que compriman y ordenen los datos. Incluso existen modelos que permiten la conexión a un televisor y una cadena de música para ver vídeos y fotos, escuchar canciones...

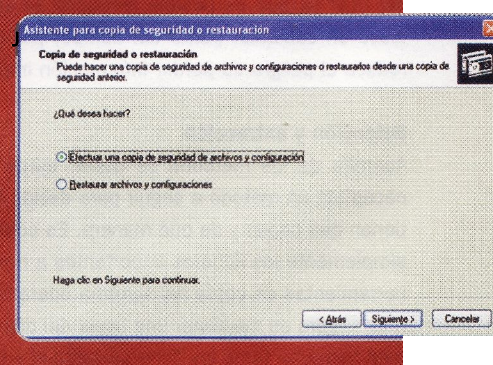
Las llaves USB no parecen una buena alternativa para realizar copias de seguridad, pero, sin embargo, pueden ser muy útiles para que llevemos encima sólo nuestros ficheros más importantes y que estén así 3 salvo.



Los discos duros externos pueden ser una buena alternativa para hacer copias de seguridad de nuestro sistema. Algunos están especialmente pensados para preservar la confidencialidad, como este modelo que sólo se activa mediante la huella dactilar del propietario.

Aplicaciones de backup

Para realizar correctamente copias de seguridad, necesitaremos instalar un programa adecuado, El software de *backup* lleva a cabo principalmente las siguientes funciones con los datos que copia. Para empezar, la compresión, cuya finalidad es que la copia de seguridad ocupe el mínimo espacio posible y se adapte a los distintos soportes. Después, la separación en volúmenes, que permite dividir la copia almacenada en varios soportes como discos. También está la programación de copias, que establece un calendario de copias para prevenir posibles problemas. La encriptación, por su parte, evita que el contenido sea analizado por terceros, mientras que la recuperación de la copia (parcial o total) puede ser completa o de todo el disco como de aquellos archivos individuales que nos interesen.



Existen diversos programas para realizar copias de seguridad. El propio sistema Windows ofrece el suyo. Obviamente, no es el que más prestaciones tiene, aunque Windows Recovery Environment de Windows Vista es bastante completo. Entre ios programas de pago (para un solo PC), encontramos los incorporados a los programas de grabación de disco, como Ñero BackUplt o el Roxio Toast, así como otros más sofisticados, como el Ventis BackupSuite 2008. Entre ios gratuitos hay que destacar Cobian Backup (www.educ.umu.se/~cobian/cobianbackup.htm) y Areca Backup (http://areca.sourceforge.com).

Los ordenadores portátiles también necesitan disponer de la posibilidad de realizar copias de seguridad en cualquier momento. Para este tipo de casos puede ser conveniente utilizar un disco duro externo portátil.

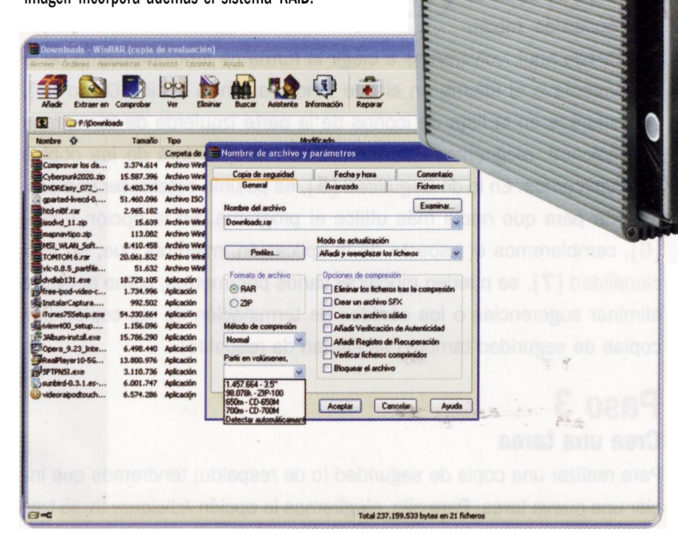
Además de los discos duros existen otras posibilidades de almacenamiento externo para guardar nuestros datos. Una de las más populares son las memorias USB. Estos dispositivos tienen la gran ventaja de tener un tamaño realmente pequeño, pero el inconveniente es que no disponen de una gran capacidad de almacenamiento. Aun así pueden resultar muy útiles para guardar una copia de ciertos documentos que no ocupen demasiado espacio, como los de texto u hojas de cálculo. Si guardamos estas copias periódicamente en una llave USB, en el caso que tengamos un problema con el ordenador, podremos acudir a otro PC y ponernos a trabajar de inmediato sin necesidad de esperar a restaurar una copia de seguridad. De la misma forma, podemos utilizar para este tipo de uso los reproductores MP3. Es posible reservar parte del espacio disponible para música y otra parte para datos y, de esta forma, llevar siempre con nosotros los archivos más importantes.

Cintas magnéticas y disquetes

Las cintas magnéticas o de *backup* han sido durante mucho tiempo el sistema de copia preferido especialmente en entornos profesionales. La razón ha sido hasta hace muy poco la excelente relación entre capacidad de almacenamiento y precio. Sin embargo, el abaratamiento de soportes como los DVD o los propios discos duros, así como los inconvenientes de las cintas han hecho que este sistema pierda terreno. Hay que tener en cuenta que para utilizarlas se necesitan dispositivos especiales. Además, se trata de un sistema secuencial de almacenamiento, por lo que el tiempo de acceso a una información concreta es alto. Por otro lado, esta característica permite que la velocidad de escritura y de lectura sea muy rápida. En cualquier caso, sigue siendo un sistema utilizado para la copia de seguridad pero destinado a grandes sistemas.

En el caso de ordenadores personales suele ser más conveniente optar por otro tipo de formatos. No podemos concluir esta lista de sistemas de almacenamiento sin mencionar a los prácticamente desaparecidos disquetes. Han supuesto durante muchos años el único método que hemos tenido a nuestro alcance para hacer copias de seguridad. En la actualidad, prácticamente ningún ordenador personal dispone de unidad de disquete y sus prestaciones y relación capacidad precio son muy malas, por lo que su uso es marginal.

Existen sistemas de almacenamiento externo que a través de protocolos como el NDAS pueden ser utilizados con sólo conectarlos a una red local. El modelo de la imagen incorpora además el sistema RAID.



Aunque lo más cómodo y recomendable para realizar copias es un buen programa de *backup*, es posible también utilizar herramientas de compresión como WinRar. Éstas permiten incluso almacenar archivos comprimidos en distintos discos o volúmenes.

Sistemas remotos

El desarrollo de la tecnología tanto de redes locales como de acceso a Internet por banda ancha ha convertido al almacenamiento remoto en una posible alternativa para realizar copias de seguridad. El sistema es sencillo, en vez de confiar en un soporte local para la copia enviaremos nuestros ficheros a través de la red para que sean almacenados en otro lugar. Como hemos apuntado, una de las posibilidades es la copia a través de ia red. Se puede realizar enviando los ficheros a un ordenador conectado que ponga a disposición espacio de almacenamiento o directamente utilizando un disco duro conectado a la red. Existen sistemas que permiten acceder a estos discos como si fueran locales.



Existen servicios en la red que permiten realizar copias de seguridad a través de Internet y mediante un software especial. De esta forma, no necesitaremos disponer de un sistema de almacenamiento para las copias y tendremos nuestros datos a salvo en otro lugar.

Tenemos distintos sistemas, como SAN o ÑAS, pero el más eficaz es el NDAS, el más rápido de funcionamiento y que soporta incluso el uso de protocolos RAID. Los sistemas de almacenamiento remoto por Internet, por su parte, deben ser contratados a un proveedor. Normalmente, utilizan un software especial proporcionado por la empresa que ofrece el servicio y funcionan contratando una determinada frecuencia de copias. Según el tipo de servicio, será posible hacer copias sólo de determinados ficheros y acceder a ellas utilizando un navegador y otros servicios. Los sistemas de almacenamiento remoto ofrecen la ventaja de la comodidad, pues no hay que estar pendientes de la copia y de protegerlos de inconvenientes que puedan afectar tanto a las éstas como a los originales de forma local, como incendios u otras catástrofes. El inconveniente es que el almacenamiento remoto es bastante más lento que el local. Por otro lado, hay que tener en cuenta que ponemos en manos de una empresa externa gran cantidad de datos que pueden ser confidenciales. Existen servicios de copia de seguridad remota de todo tipo, y no sólo para entornos empresariales. Es posible contratar estos servicios también para nuestro ordenador personal.

Haz el backup tú mismo



Te enseñamos a hacer copias de seguridad con el programa Cobian Backup 8

No se trata tanto de poner a salvo el sistema operativo y los programas sino nuestros documentos. Nadie está libre de que pueda pasar algo con sus datos, por muy bueno que sea el antivirus y por muchas precauciones que tome para cuidar sus discos.

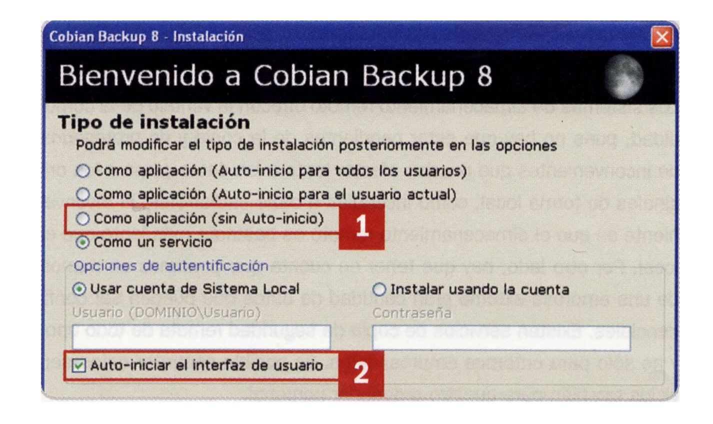
Software incluido en el DVD

Cobian Backup 8
Herramienta gratuita para hacer copias de seguridad
Ubicación
Laboratorio PCA/Guía práctica

Para realizar con eficacia una copia de seguridad es necesario utilizar el software adecuado. Muchas *suites* de grabación incorporan en el paquete un programa que permite realizar *backups,* pero suele ser bastante sencillo y orientado a las copias de discos. Además, algunas funciones puede que no estén disponibles. Se trata de un caso parecido al de la herramienta de *backup* de Windows, que puede sacarnos de algún apuro, pero no tiene la eficacia de un programa diseñado para este fin. En este caso, vamos a utilizar una herramienta gratuita, pero existen muchos programas en el mercado que realizarán perfectamente esta tarea. Hay que tener en cuenta que la aplicación de *backup* que nos ocupa, Cobian Backup 8, no realiza copias directas a CD o DVD, aunque sí es posible hacerlas sobre un directorio del disco y, luego, pasarlas a estos soportes. Sin embargo, resulta muy útil si disponemos de un disco duro externo o para copiar a otro equipo de la red local. Es más, contiene todas las funciones de programas de *backup* más «serios», por lo que servirá para comprender el funcionamiento de éstos.

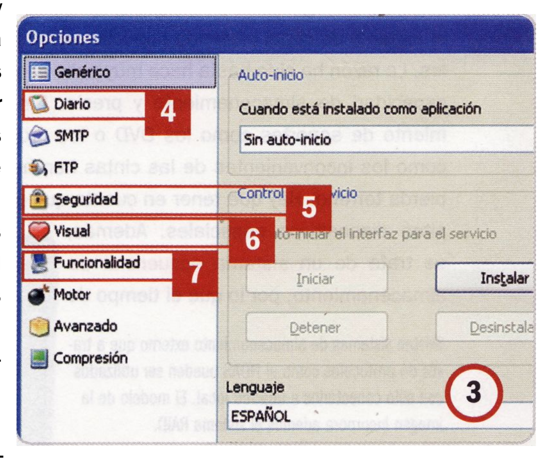
Paso 1
Descarga e instalación

En primer lugar, nos conectaremos con la página web del desabollador del programa Cobian en www.educ.umu.se/-cobian/cobianbackup.htm o acudiremos al DVD que acompaña a este número de PC Actual y en el que le hemos incluido. Una vez hecho, se iniciará la descarga y tendremos un ejecutable, con lo que, para iniciar el proceso, sólo hemos de hacer clic en el icono correspondiente al fichero que acabamos de bajarnos. Elegiremos el idioma español y continuaremos pulsando Ok. Tras leer el consabido documento de las condiciones de la licencia y escoger la carpeta donde queremos que se instale el programa, pasaremos a una ventana en la que se nos pedirá cómo queremos que funcione. Por defecto, el software arrancará como servicio, es decir, pasará a formar parte de los programas que se inician con el sistema operativo. Es la mejor forma de que funcionen correctamente las copias periódicas. Si, por el contrario, sólo queremos hacer duplicados puntuales, elegiremos la opción Como aplicación (sin Auto-inicio) [1]. En el resto de posibilidades, el programa se iniciará automáticamente en la cuenta que escojamos. También es posible elegir si queremos o no que se inicie la interfaz de usuario [2] cuando se cargue el programa. Una vez seleccionadas las opciones, pulsamos en Siguiente.



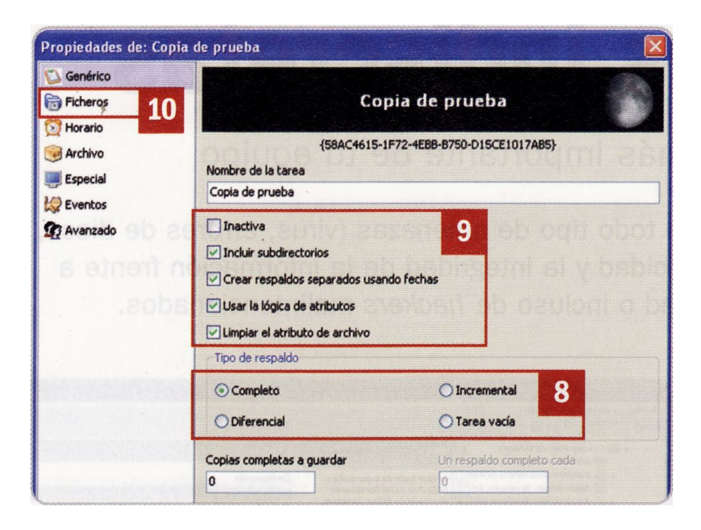
Paso 2
Opciones del programa

Tras la instalación, se ejecutará y pasará a formar parte de los iconos de la parte inferior derecha de la pantalla de Windows. Éste tiene la forma de una medialuna negra. Para acceder al mismo, haremos doble clic en dicho icono y se presentará una ventana con varios menús. En primer lugar, configuraremos las opciones que ofrece el programa; para ello haremos clic con el ratón en el menú Herramientas y, a continuación, en Opciones [3]. Aparecerá entonces una pantalla con aquellas que podemos modificar. Desde aquí, volveremos a elegir la forma de funcionamiento de la herramienta o el idioma en el que funciona. En la opción Diario [4], que aparece en la lista de iconos de la parte izquierda de la ventana de opciones, elegiremos qué información se guardará de las copias que realicemos. En la de Seguridad [5], es posible establecer una contraseña para que nadie más utilice el programa. En la opción Visual [6], cambiaremos el aspecto de la aplicación, mientras que, en Funcionalidad [7], se pueden modificar vahos parámetros, como activar o eliminar sugerencias o los sonidos de terminación de las copias (las copias de seguridad también se llaman de respaldo).



Paso 3
Crea una tarea

Para realizar una copia de seguridad (o de respaldo) tendremos que iniciar una nueva tarea. Para ello, elegiremos la opción Adicionar tarea tras abrir el menú Tarea haciendo clic con el ratón. Aparecerá una pantalla parecida a la del Paso 2 en la que podremos configurar las características de la tarea de copia de respaldo. Lo primero que hay que hacer es



escoger qué tipo de copia de seguridad queremos realizar. Se nos presentan las opciones siguientes: Completo, Incremental, Diferencial o Tarea vacía [8]. La primera realizará una copia de todos los datos, la segunda irá copiándolos a medida que se vayan almacenando en el soporte y la tercera sólo copia los ficheros que han cambiado. La última opción no contiene ficheros, pero puede utilizarse para realizar ciertas tareas. Para más detalles sobre los tipos de tareas de copia de seguridad, hay que consultar la introducción en el apartado correspondiente. En éste, también podremos definir el número de copias a realizar y otros detalles, como la inclusión de subdirectorios o la limpieza de atributos de los archivos [9]. En el apartado Ficheros [10], elegiremos qué archivos o carpetas del disco queremos copiar. Podemos arrastrarlos y soltarlos o pulsar en el botón Adicionar para agregar los ficheros que queramos. Como peculiaridad, el programa deja agregar servidores FTP, de los que haremos una copia de seguridad desde nuestro ordenador. En la parte inferior, indicaremos las carpetas de destino donde queremos que se almacenen las copias. También permite realizarlas en servidores FTP. Es posible agregar más de un destino, por lo que tendremos dos copias de seguridad en dos soportes distintos con una sola operación.

Paso 4

Programa las copias

Una de las características más importantes de una herramienta de *backup* es la posibilidad de programar las copias de seguridad de forma que éstas se realicen automática y periódicamente. En nuestro caso, activando el apartado horario, escogeremos la periodicidad de las copias. Éstas se realizaran con la frecuencia indicada sin necesidad de nuestra intervención, siempre que el programa esté activado. La aplicación ofrece todas las opciones posibles, desde los días de la semana hasta horas y fechas concretas pasando por un intervalo de tiempo en minutos. Si queremos hacer una copia inmediatamente, marcaremos la opción Único [11]. Hay

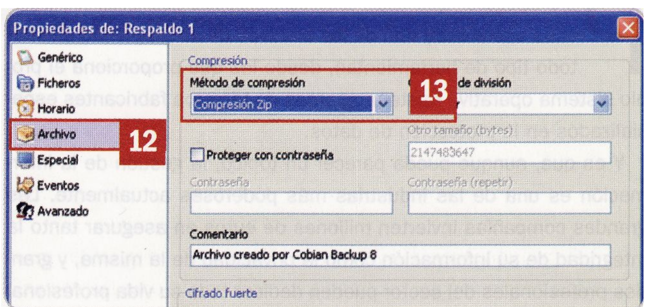


que asegurarse que en el momento que se vayan a realizar las copias se encuentren disponibles los soportes de destino que hemos elegido en el apartado anterior.

Paso 5

Encriptación y compresión

Por defecto, este programa no realiza ninguna operación de compresión ni encriptación de las copias, por lo que, para recuperar una, sólo tendremos que copiarla del soporte donde se encuentre al original. Sin embargo, ofrece la posibilidad de encriptar y comprimir, lo que ralentiza el proceso, pero añade seguridad y ahorra espacio. Al

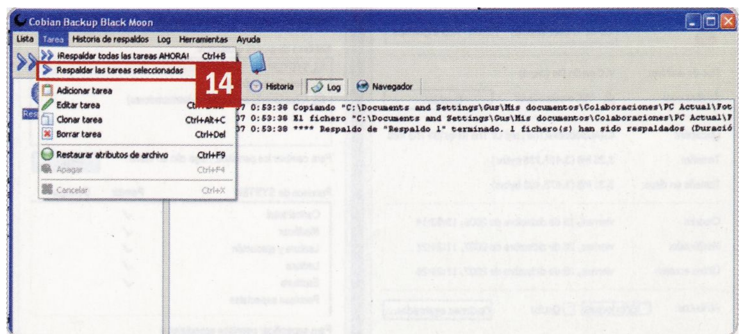


activar la opción Archivo [12], en el apartado Métodos de compresión [13], podremos escoger entre el sistema ZIP o el SQX. Dentro de cada una, es posible elegir un tamaño para los ficheros comprimidos. Resulta útil si, a continuación, vamos a grabar esos archivos en un soporte CD o DVD. También es posible elegir proteger el fichero con una contraseña para que no pueda ser abierto por terceros o que los ficheros de la copia de respaldo se encuentren protegidos por una clave de cifrado. Disponemos de cuatro sistemas distintos para proteger nuestros datos. Si ciframos o comprimimos las copias, para recuperarlas más adelante tendremos que acceder al menú Herramientas y elegir las opciones Descifrado y llaves o Descompresor, según sea el caso.

Paso 6

Otras opciones

Antes de dar inicio a la copia, podemos elegir otras opciones. En el apartado Especial, nos permite incluir o excluir cierto tipo de ficheros o algunos concretos de las copias. En Eventos, es posible ejecutar determinadas tareas antes de la copia, como cerrar o ejecutar determinados programas. Una vez creada la tarea, ésta aparecerá en la



parte izquierda de la ventana del programa. Si hacemos clic sobre ella, la ejecutaremos utilizando el comando Respaldar las tareas seleccionadas del menú tarea [14]. De esta forma, se pondrá en marcha la copia. Cuando finalice, veremos el resultado en la ventana de información de la parte derecha.

Libre de miradas indiscretas

Cómo mantener a salvo la información más importante de tu equipo

Las copias de seguridad protegen los datos frente a todo tipo de amenazas (virus, errores de disco, borrados accidentales...) pero no garantizan la privacidad y la integridad de la información frente a otros usuarios del mismo ordenador, de la misma red o incluso de *hackers* malintencionados.

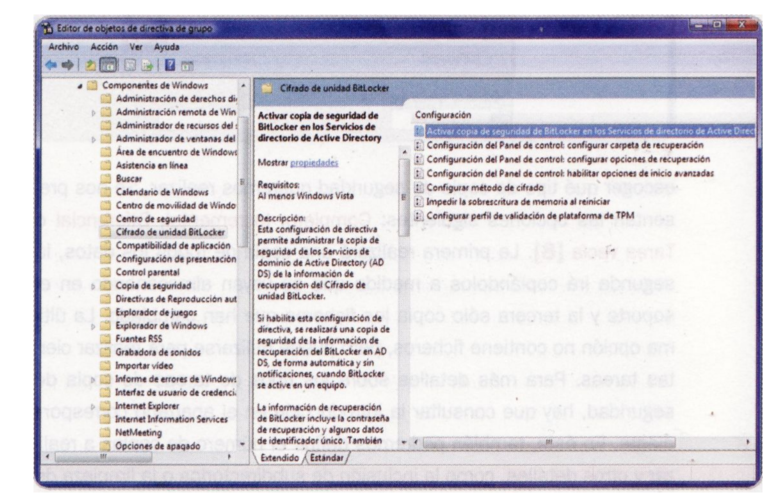
Para asegurar que cada propietario pueda gestionar los derechos sobre cada uno de los archivos de su propiedad existen todo tipo de herramientas, desde las que proporciona el propio sistema operativo hasta programas de terceros fabricantes especializados en la protección de datos.

Y es que, aunque pueda parecer un tópico, la gestión de la información es una de las industrias más poderosas actualmente. Las grandes compañías invierten millones de euros en asegurar tanto la integridad de su información como la privacidad de la misma, y grandes profesionales del sector pueden dedicar toda su vida profesional al desarrollo de este único aspecto de la informática.

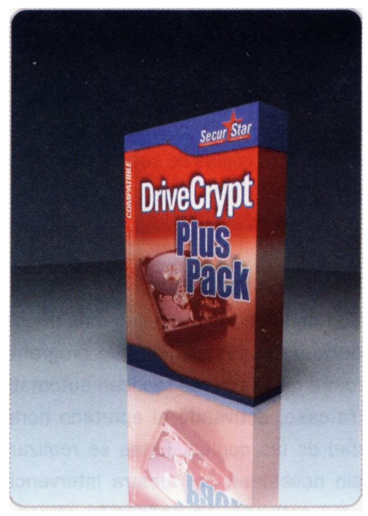
La importancia de la seguridad de los datos es tan alta que prácticamente todos los sistemas operativos diseñados incluyen sistemas para determinar la autoría de cada archivo y las operaciones que cada usuario puede realizar con este objeto. Por supuesto, Windows, el sistema operativo más utilizado del mundo, también cuenta con estas herramientas integradas en su propio núcleo.

Herramientas del sistema

Como decíamos, Windows dispone desde sus primeras versiones de las herramientas necesarias para proteger con bastante efectividad los datos. Siempre se ha basado, como la mayoría de plataformas, en un sistema integrado de gestión de derechos que permiten a los usuarios crear sus propias políticas relacionadas con el uso y creación de los documentos. Casi todos los usuarios los conocen como atributos del archivo o carpeta y sus opciones de seguridad son accesibles con sólo abrir las propiedades de cada objeto. Desde esta ventana también se puede acceder al sistema de encriptación de archivos y directorios. Esta herramienta proporciona un nivel superior de seguridad al sistema de archivos, pero ralentiza el acceso a la información y es imprescindible el uso de NTFS.

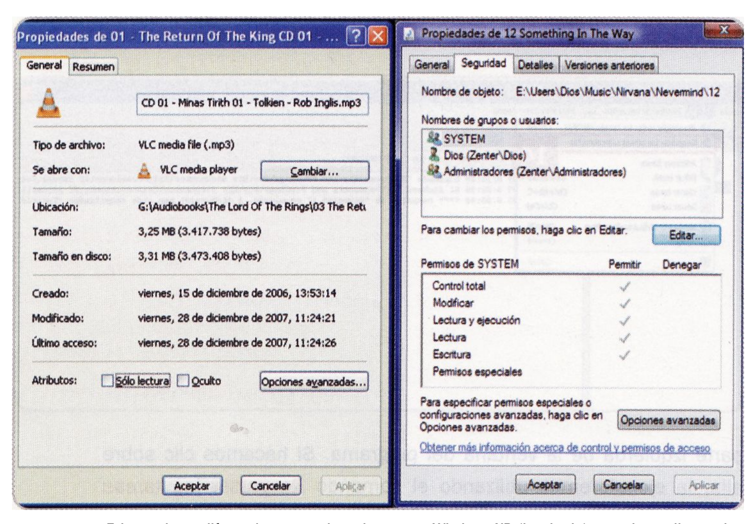


Activar el sistema de cifrado de datos basado en hardware TPM de Windows Vista no es una tarea sencilla sin un buen manual de usuario, ya que será necesario configurar servicios básicos del sistema para su correcto funcionamiento.

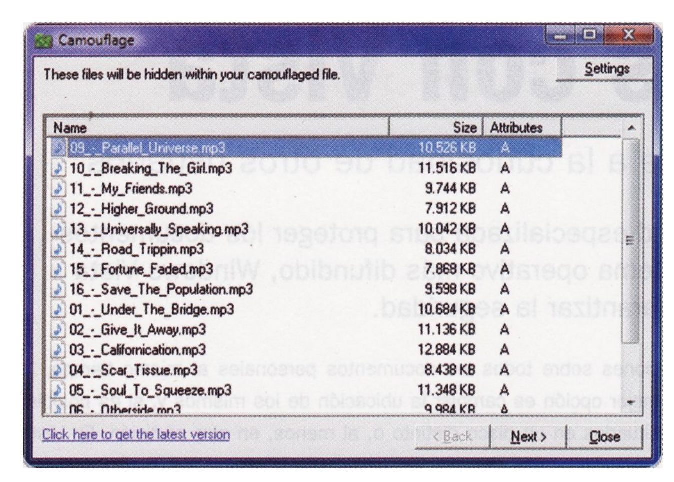


Este tipo de aplicaciones permiten asegurar todo el contenido del disco duro de cualquier equipo sin necesidad de grandes conocimientos de encriptación y sin dedicar gran parte de los recursos del ordenador a la seguridad.

La última versión del sistema operativo de Microsoft, Vista, incluye una serie de avances a este sistema básico de protección de la información. En primer lugar, mejora la gestión de los derechos de cada archivo gracias a un sistema de atributos más completo. De entre todos ellos destacan los permisos especiales que permiten desde una gestión inteligente por grupos hasta un novedoso sistema de auditoría que permite controlar las operaciones no deseadas realizadas sobre un archivo o una carpeta. Pero todas estas protecciones se realizan a nivel software, por lo que un usuario avanzado podría vulnerar la seguridad con relativa facilidad. Para aumentar el nivel de seguridad, Windows Vista es compatible con los chips TPM (Módulo de Plataforma Segura) que se incluyen en algunas placas bases. Estos integrados ofrecen encriptación para los sectores del disco duro y además verifican, cada vez que se inicia el sistema operativo, que no ha sido atacado *off-line*-, es decir, que el atacante no ha ini-



Existen claras diferencias entre el modo en que Windows XP (izquierda) trata los atributos de un archivo a como lo hace Windows Vista (derecha). El segundo permite una gestión avanzada de la seguridad de manera intuitiva.



La herramienta más utilizada actualmente para camuflar archivos bajo otro formato es Camouflage, disponible desde http://camouflage.unfiction.com.

ciado el equipo con otro sistema operativo para conseguir el control. Si el ordenador ha sufrido uno de estos ataques, arranca el sistema de recuperación para regresar a un estado de máxima seguridad. Este sistema es un complemento perfecto a la gestión de derechos, pero si el ordenador falla o el disco duro es instalado en otro PC y, además, la clave de recuperación no se encuentra, se pueden perder de manera definitiva los datos. En todos estos casos, la información puede ser accesible por otros usuarios con cuenta de administrador en el equipo, por lo que se puede recurrir a otras herramientas, ajenas al sistema operativo, capaces de gestionar la protección de los datos con sistemas de encriptación prácticamente inviolables.

Software de encriptación

La instalación y la configuración del software de encriptación nunca han sido una tarea fácil. Consideradas como herramientas para profesionales, han evolucionado para que su uso esté al alcance de todos los usuarios. Ahora, las opciones de configuración son más intuitivas sin perder un ápice de seguridad.

Aplicaciones como PGP Whole Disk Encryption o SecurStar DriveCrypt Plus encnptan archivos o carpetas integrándose en el sistema, pero su mayor ventaja es que son capaces de cifrar el disco duro y todo su contenido. Esta función resulta casi transparente para el usuario ya que se asocia a las cuentas de usuario de Windows y encripta automáticamente todos los archivos que se utilizan. También se integran a la perfección con todo el sistema de modo que, cuando se envía un archivo codificado por correo electrónico, estas aplicaciones transcriben los datos adjuntos para que el receptor del mensaje pueda manejar los documentos con toda libertad.

Tradicionalmente, este tipo de aplicaciones han ralentizado los ordenadores considerablemente ya que se necesitan resolver complicados algoritmos para encriptar cada archivo. Sin embargo, las técnicas actuales permiten que los recursos consumidos sean mínimos y, por tanto, que el rendimiento de los equipos apenas sufra disminución alguna. Se trata, por tanto, de la opción que ofrece mayor seguridad para los usuarios de ordenadores portátiles, ya que la información estará a salvo de otros usuarios incluso si pierde el equipo o sufre un robo.

Existen otras aplicaciones, en su mayoría de distribución gratuita o con licencia Shareware, que ofrecen otros métodos de proteger la información sin involucrar directamente al sistema operativo. Scramdisk es una potente utilidad de encriptación que permite reservar entre 50 Mbytes y 2 Gbytes de espacio en el disco duro para crear una unidad virtual encriptada accesible desde Mi PC. Esta nueva unidad está protegida por una clave y permanece codificada en todo momento. Como esta aplicación es de código abierto, sus algoritmos se actualizan casi constantemente por lo que la seguridad se incrementa cada vez que se actualiza a una nueva versión.

También existen soluciones hardware para aumentar la seguridad de los datos más sensibles. Empresas como SanDisk o CryptoStick han diseñado discos duros externos que incluyen algoritmos hardware de encriptación que permiten proteger la información frente a robos y pérdidas. Los sistemas de seguridad de estos dispositivos se complementan con equipos biométricos basados en la lectura de huellas digitales o el típico cuadro de diálogo para la introducción de claves.

La técnica del camaleón

La mayoría de los formatos de archivos tienen información redundante o campos que no se suelen utilizar. Estos bytes de información se pueden usar para insertar otros archivos de modo que desaparezcan en su interior. Por ejemplo, los archivos JPEG, MP3 o DOC no alteran su funcionamiento si se añade información extra al final del fichero. Si esta información está encriptada pasará desapercibida para la mayoría de usuarios. Esta técnica puede utilizarse para ocultar archivos a otros usuarios del mismo ordenador o para proteger la información que se envía a través de Internet. Para utilizar de forma efectiva esta técnica se suelen emplear dos tipos de programas: uno que se encarga de insertar los datos confidenciales en otros documentos de formato distinto y otro que es capaz de extraer la información oculta. Se podría considerar un tipo de esteganografía (rama de la criptología que trata sobre la ocultación de mensajes), pero la mayoría de los expertos en seguridad no la incluyen entre sus técnicas, entre otras razones porque siempre ha estado relacionada con la ocultación de todo tipo de amenazas de seguridad como los *rootkits*, *spyware* o la distribución de copias ilegales de software.

Algunos llaveros USB y discos duros incluyen sistemas de encriptadc |ue se apoyan en técnicas biométricas para asegurar al máximo los datos que contienen.

Sólo algunas placas bases cuentan con un chip TPM (módulo de plataforma segura) para encriptar los datos de sus discos duros a nivel hardware.

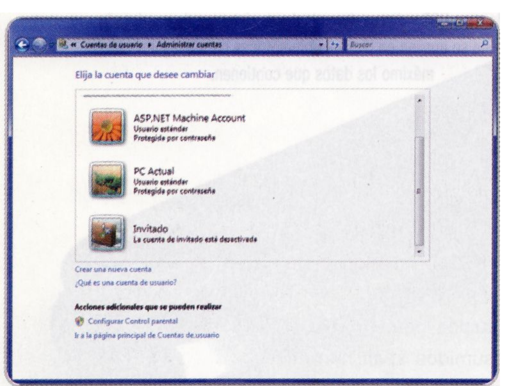
Datos blindados con Vista

Protege tus documentos personales frente a la curiosidad de otros usuarios

No es imprescindible recurrir a una *suite* de seguridad especializada para proteger los documentos personales. Al igual que versiones anteriores del sistema operativo más difundido, Windows Vista proporciona un buen número de herramientas para garantizar la seguridad.

Como todo sistema operativo, Windows Vista ofrece herramientas para garantizar la gestión segura de los archivos privados de los usuarios. Algunas de estas funciones, como BitLocker, necesitan hardware especial compatible con la plataforma TPM, pero la mayoría de opciones de seguridad se basan en software y están disponibles para todos los usuarios del sistema operativo de Microsoft. Para que los datos personales de todos los usuarios de un ordenador estén seguros y fuera del alcance de otras personas, sólo es necesario combinar las prestaciones que ofrecen la gestión de cuentas y la encriptación con algunos pequeños trucos de organización de información.

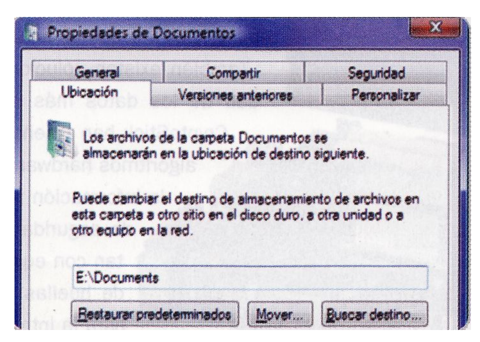
Paso 1
Gestiona cuentas



La mayoría de los ordenadores domésticos y muchos de los que se encuentran en pequeñas empresas se comparten entre varios usuarios. Esto puede provocar problemas de privacidad e integridad de los datos. La solución propuesta por Windows es utilizar cuentas independientes para cada usuario. De este modo, la información de cada persona está protegida frente a posibles «errores» de otros usuarios y sólo el administrador del equipo podrá acceder a los datos. Desde el Panel de control de Vista seleccionaremos Cuentas de usuario y Administrar otra cuenta con el objetivo de crear una nueva para cada usuario del ordenador. El siguiente paso consiste en pulsar el enlace Crear una nueva cuenta con la opción Usuario estándar activada y pulsar el botón Crear cuenta. El siguiente paso fundamental es hacer clic sobre el icono de la nueva cuenta y seleccionar el enlace Crear una contraseña. Tras rellenar los campos correspondientes sólo basta pulsar el botón Crear contraseña.

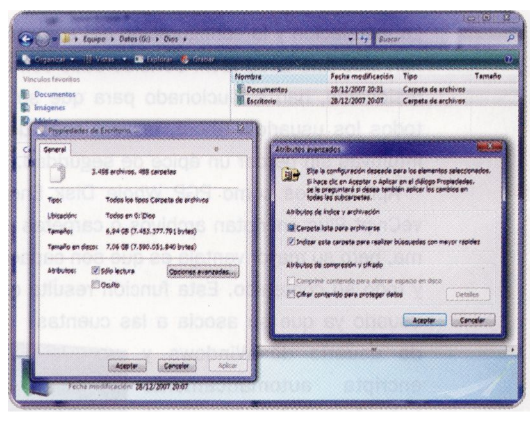
Paso 2
Carpetas personales agrupadas

La mayoría de los usuarios almacena sus documentos personales en carpetas alojadas en el escritorio o en los directorios especiales de Mis documentos situados en el menú de inicio o en el propio escritorio. Windows sitúa estas carpetas dentro de su propia estructura de directorios, por lo que gestionarlos como una única entidad no resulta cómodo. Para realizar operaciones sobre todos los documentos personales al mismo tiempo, la mejor opción es cambiar la ubicación de los mismos y, si es posible, situarlos en un disco distinto o, al menos, en otra partición. En Vista para cambiar la posición de los archivos personales tendremos que localizar las carpetas. Éstas se encuentran normalmente en C:\Usuarios, organizadas según las distintas cuentas creadas en el equipo. Ahora basta con acceder a la carpeta del usuario en cuestión y hacer clic con el botón derecho del ratón sobre la carpeta Documentos. En el siguiente menú contextual tendremos que elegir Propiedades y, posteriormente, seleccionar la pestaña Ubicación. El siguiente paso es cambiar la ruta de esta carpeta y pulsar sobre el botón Mover. Para terminar hay que repetir estos pasos con todas las carpetas que queramos cambiar de ubicación.



Paso 3
Asegurados bajo llave

En la mayoría de sus versiones, Vista utiliza el sistema de cifrado EFS que ofrece un nivel de seguridad más que suficiente para cualquier usuario doméstico o pequeñas empresas. Esta herramienta de encriptación se puede utilizar para proporcionar un nivel de seguridad extra a los documentos personales de cada usuario. Gracias al anterior paso, en el que se han organizado todos las carpetas de usuario (Escritorio, Documentos...), en una partición independiente el proceso es aún más sencillo.



Para encriptar los datos de un usuario, hay que seleccionar las carpetas que se quieren cifrar y pulsar el botón derecho del ratón para abrir las propiedades de éstos. Después sólo tendremos que pulsar el botón Opciones avanzadas para acceder a la configuración de cifrado. Tras marcar la casilla Cifrar contenido para proteger datos pulsaremos en Aceptar por dos veces. A continuación, marcaremos la opción Aplicar cambios a los elementos seleccionados y a todas las subcarpetas y archivos. En este punto, Windows Vista procederá a establecer la encriptación de los archivos lo cual puede tardar aproximadamente unos 20 minutos por cada «giga» de información (depende de la velocidad del ordenador y del tipo de archivos más utilizados). Si se repiten estos pasos para cada usuario de un ordenador todos los archivos personales están organizados y encriptados sin necesidad de recurrir a software de terceros.

Seguridad con PGP Desktop

Consigue que tus discos y particiones se cifren en apenas unos segundos

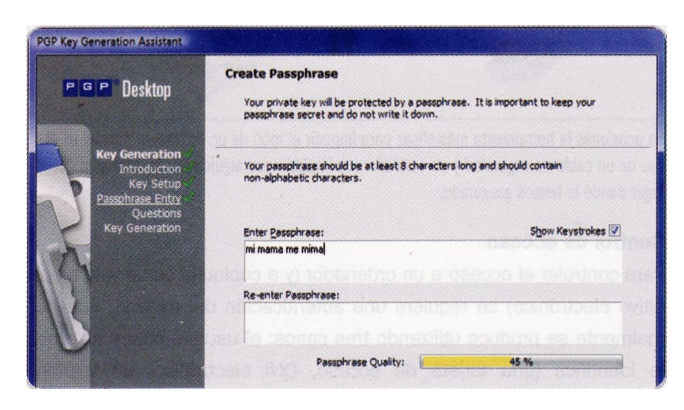
Suites de protección de datos como PGP Desktop disponen de aplicaciones capaces de cifrar discos enteros de manera transparente para el usuario y, lo que es más importante, sin que el rendimiento del equipo se resienta.

Con esta *suite* se pueden gestionar todos los aspectos del cifrado de documentos que puede necesitar un usuario doméstico. En este caso aprenderemos a configurar una unidad virtual cifrada y a encriptar una partición completa con claves de 256 bits.

Paso 1

Instala y crea una clave

La instalación es la habitual y sólo hay que seleccionar el idioma (lamentablemente, el programa aún no está en castellano). Una vez iniciada la sesión aparecerá el asistente de configuración pero para este caso tendremos que cerrarlo. El programa se inicia automáticamente con el sistema, por lo que siempre está presente un icono (con forma de candado) en la barra de herramientas. Haz doble clic sobre el mismo para mostrar la interfaz de la aplicación.

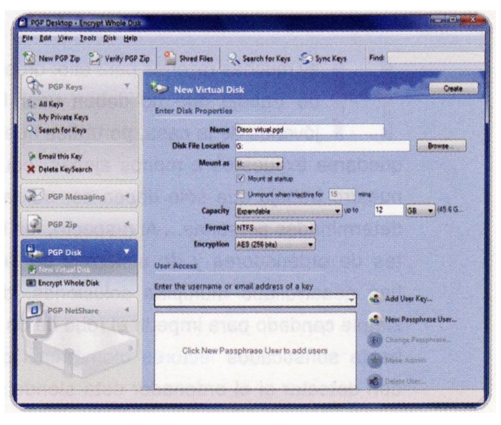


El primer paso es crear una clave de cifrado de datos para asegurar el cifrado de datos y su posterior recuperación en caso de error fatal del sistema. Para ello basta con seleccionar File en el menú superior, New y PGP Key. Esta acción abrirá el asistente de generación de claves. Hay que rellenar dos campos: el primero es el nombre completo y el segundo una dirección de correo electrónico. Es obligatorio rellenarlos porque cada clave del sistema debe estar asociada a un usuario. A continuación hay que introducir la frase de codificación. En la parte inferior una barra indica la eficacia de la frase escrita para generar claves. Evitar repeticiones de caracteres aumenta la seguridad de la misma. Una vez escrita y repetida pulsaremos Siguiente y después podremos pulsar Skip para evitar alargar demasiado el proceso de generación de claves. Ya estará generada la clave.

Paso 2

Crea un nuevo disco virtual

Selecciona PGP Disk en el menú lateral de la aplicación y se expandirán las dos funciones que nos interesan. Para este paso elegiremos la opción New Virtual Disk. En este punto tendremos que rellenar todos los campos: nombre de la unidad, destino del archivo físico para la unidad virtual, letra asignada, capacidad, formato y encriptación. Es recomendable marcar la opción Mount at startup y desmarcar Unmount when inactive para que la unidad esté siempre activa. Del mismo modo también es recomendable seleccionar el formato NTFS por razones de compatibilidad y rendimiento. Por último hay que añadir una* clave para gestionar el acceso a la unidad virtual. Basta pulsar en el botón Add User Key, seleccionar la clave que acabamos de crear y pulsar los botones Add y OK en este orden. Finalizaremos presionando el botón Create situado en la parte superior de la ventana.

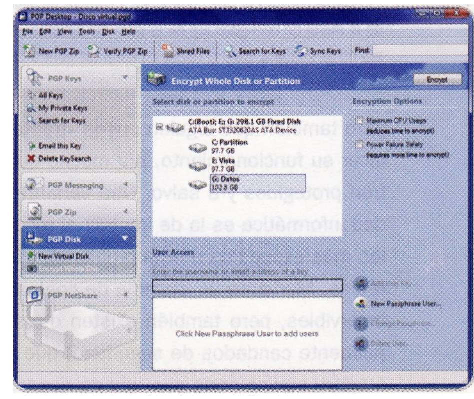


Paso 3

Encripta un disco por completo

Esta *suite* también permite encriptar un disco completo. En realidad no es necesario cifrar todo el disco ya que también trabaja sobre particiones. Para empezar, seleccionaremos de nuevo PGP Disk y, en este caso, elegiremos la opción Encrypt Whole Disk. La ventana principal cambiará para mostrar una lista expandible con todos los discos instalados en el equipo y sus respectivas particiones. En este caso sólo vamos a encriptar una partición, por lo que hay que expandir la unidad principal del sistema y seleccionar el objetivo con un simple clic de ratón. La opción Power Failure Safety ofrece un nivel de seguridad extra ya que protege la unidad encriptada frente a fallos críticos del sistema durante los procesos de cifrado. Es interesante marcarla si la información es especialmente relevante o si no se realizan copias de seguridad con suficiente frecuencia. El último paso es seleccionar la clave para la encriptación. No se puede utilizar la clave generada en el primer paso, por lo que habrá que generar una nueva o recurrir a la del sistema (más recomendable para garantizar el acceso del usuario frente a errores graves del sistema).

Para fijar la contraseña hay que pulsar el botón New Passphase User, seleccionar User Windows Password y pulsar dos veces el botón Next. Por último, introducir la clave del sistema, avanzar por el asistente hasta su finalización y pulsar el botón Encrypt situado en la parte superior de la ventana principal.



El PC como una caja fuerte

Logra que tu equipo se vuelva invulnerable ante cualquier amenaza

Ya hemos visto la importancia que tiene proteger nuestros datos, ya sea de la posibilidad de que se pierdan o deterioren o de que alguien acceda a ellos sin nuestra autorización. Sin embargo, a veces necesitaremos también proteger el uso de nuestro propio ordenador.

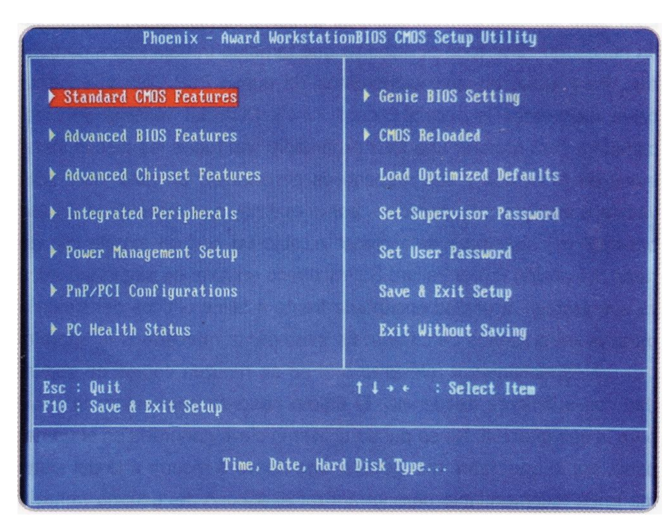
Hay muchas razones para ello: ordenadores de trabajo que no deben usar los más jóvenes de la casa, portátiles que pueden quedarse expuestos a manos ajenas, equipos en nuestro trabajo que sólo deben ser utilizados por determinadas personas... Al respecto, los fabricantes de ordenadores y de sistemas de seguridad han desarrollado múltiples soluciones, desde el simple candado para impedir el robo de un portátil, hasta sofisticados lectores biométricos que pueden detectar si el ordenador está siendo utilizado por alguien no autorizado.

Dentro de la seguridad informática, limitar el uso del ordenador puede considerarse el primer paso y quizás el más drástico, y es una preocupación que existe desde hace mucho tiempo. No en vano las BIOS de los ordenadores personales, el programa de arranque básico (lo primero que ejecuta el ordenador al encenderse), contemplan la posibilidad de establecer una contraseña. Esto impide que alguien que no conozca dicha contraseña pueda acceder a nuestros datos, pero también que alguien pueda «trastear» con el ordenador y perjudicar su funcionamiento, por mucho que nuestros datos se encuentren protegidos y a salvo. Otra variante de esta faceta de la seguridad informática es la de impedir el robo de ordenadores, sobre todo los más expuestos a este problema, como son los ordenadores portátiles. Mediante un sistema de contraseña o reconocimiento serán inservibles, pero también existen otras protecciones físicas (principalmente candados de seguridad) que pueden sernos de utilidad si nuestro equipo corre ese tipo de riesgos.



Aunque aún no se encuentran disponibles comercialmente para usuarios personales, los aparatos de reconocimiento de iris ya se utilizan en situaciones en las que la seguridad es muy importante, como en misiones militares como la de la imagen.

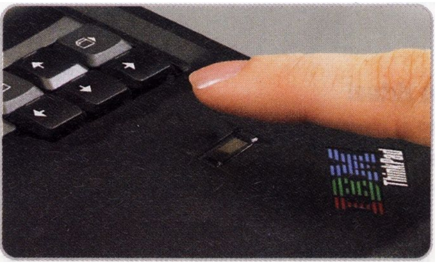
En ocasiones la herramienta más eficaz para impedir el robo de un ordenador portátil es el uso de un cable de seguridad y un candado que impidan que alguien pueda llevárselo del lugar donde lo hemos asegurado.



Es posible establecer una contraseña y nombre de usuario para utilizar nuestro PC accediendo al menú de configuración de la BIOS del sistema. Hay que tener en cuenta que este sistema no es infalible, pero sí eficaz en entornos controlados.

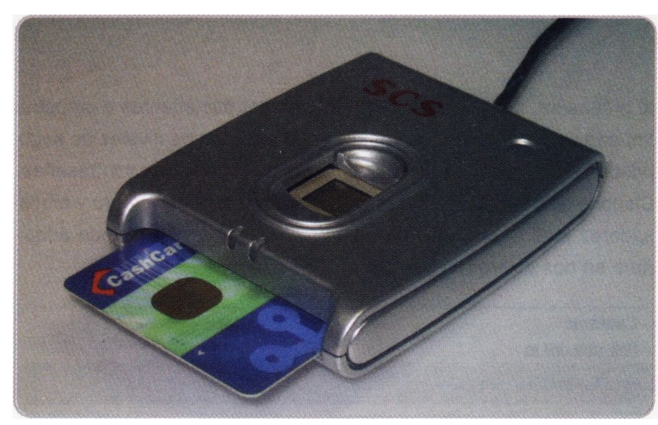
Control de acceso

Para controlar el acceso a un ordenador (y a cualquier sistema o dispositivo electrónico) se requiere una autenticación del usuario, que normalmente se produce utilizando tres casos: el usuario posee algo que le identifica (una tarjeta de acceso, DNI electrónico, un teléfono móvil...); el usuario conoce algo que lo identifica (usuario y palabra clave, su número de DNI...), o el usuario puede identificarse con parte de su cuerpo (huellas digitales, reconocimiento facial...). En sistemas en los que se precisa una mayor seguridad, como en instituciones gubernamentales, se utiliza más de un tipo de autenticación para asegurar al máximo la identidad del usuario. El segundo caso de autenticación es quizás el más clásico y el más utilizado. Como hemos comentado antes, los ordenadores disponen en su BIOS un sistema que les permite controlar quién está accediendo al ordenador. Para activarla en primer lugar tendremos que acceder a la configuración de la BIOS pulsando la tecla correspondiente. Una vez accedamos al menú de configuración, podremos establecer la palabra clave. Se trata de un sistema, sin embargo, que no es demasiado seguro porque hay diversos



Algunos ordenadores portátiles ya disponen de su propio sistema de reconocimiento de huellas dactilares. Se puede configurar el equipo de manera que sólo pueda ser utilizado por usuarios de los que pueda reconocer las huellas.

métodos para saltarse esa protección, en parte por el peligro que supone olvidarse de la palabra clave y no poder utilizar el PC aunque seamos los propietarios. En cualquier caso, puede ser un sistema efectivo para un entorno en el que no precisemos un nivel alto de seguridad, por ejemplo para un ordenador personal en nuestra casa. Establecer un nombre de usuario y una contraseña en el sistema operativo es menos efectivo, pues con un disco de arranque cualquier persona podría acceder a nuestro ordenador y a todos los datos que contuviera. En esos casos, y si el entorno no es seguro, es conveniente instalar ordenadores sin unidades de discos, o con unidades protegidas con candados u otros sistemas de seguridad.



Algunos sistemas permiten la identificación simultánea mediante dos métodos para aumentar la seguridad. El dispositivo de la imagen permite identificar tanto mediante tarjeta como utilizando un escáner de huellas digitales de forma simultánea.

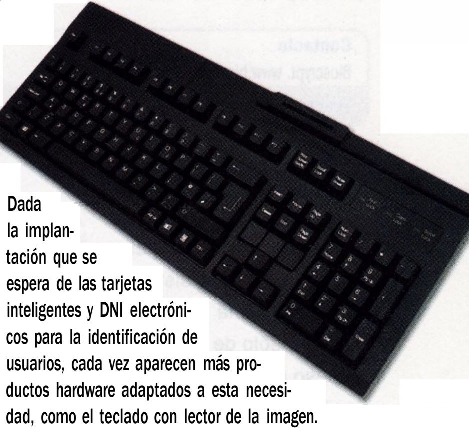
Algunos sistemas, como el que se ofrece en la página web www.Idcontrol.net, se basan en el comportamiento del usuario al teclear. Recogen las características de este comportamiento y luego son capaces de identificar al usuario autorizado mediante estos parámetros.

Identificadores

Como hemos mencionado, uno de los métodos para identificar a un usuario es entregarle una tarjeta identificativa o basarse en algo que posea y que le identifique, como el DNI o el teléfono móvil. La reciente implementación en España del DNI electrónico (más detalles en el recuadro adjunto) ofrece una solución interesante a este respecto. En la actualidad este sistema se utiliza para identificación en páginas y servicios web de la administración, pero es posible desarrollar aplicaciones para el control de acceso a ordenadores mediante un lector específico. Además del DNI electrónico se utilizan otro tipo de tarjetas llamadas inteligentes que se fabrican con un chip especial difícil de duplicar. También se utilizan para otras aplicaciones tarjetas magnéticas (parecidas a las de crédito) que sin embargo son más fáciles de duplicar o copiar. Hay que tener en cuenta que este sistema de identificadores tiene el inconveniente de que cualquier persona que se haga con uno de estos identificadores puede acceder al ordenador o al sistema protegido.

Sistemas biométricos

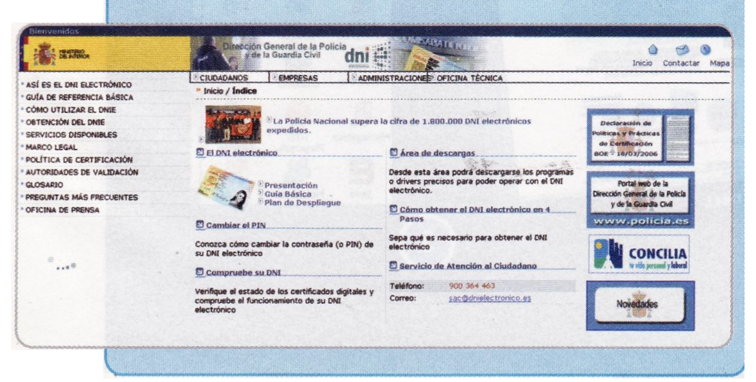
Los sistemas de reconocimiento por partes o características del cuerpo humano como la hueiia dactlar o la propia cara han pasado en unos años directamente desde la ciencia ficción a nuestros ordenadores. Ya existen diversos modelos de portátiles, sin ir más lejos, que adoptan sensores de huellas para permitir el uso del equipo. Otros sistemas biométricos como el reconocimiento facial, de la forma de la mano o del iris se utilizan en entornos más avanzados y menos comerciales. Dentro de la biometría también existen otros sistemas de reconocimiento basados más en el comportamiento que en características físicas. Uno de los más interesantes es el que detecta una forma determinada de teclear en el ordenador (ritmo, presión...). Otro más clásico es el escáner de firmas, pero resulta costoso y en ocasiones poco fiable. Finalmente el reconocimiento de voz completa los principales sistemas biométricos aplicados hoy en día. En cualquier caso, y por seguro que sea el método de acceso, el nivel de seguridad dependerá en gran parte de lo cuidadosos que seamos nosotros mismos. Si utilizamos contraseñas, procurar que éstas sean largas y difíciles de adivinar; si empleamos tarjetas de acceso llevarlas siempre encima o dejarlas en lugar seguro. Con los sistemas biométricos no es necesario ser tan cauteloso, pero siempre estaremos expuestos a descuidos como el de dejar el ordenador encendido o sin proteger. No existe tecnología capaz de paliar un descuido.



Dada la implantación que se espera de las tarjetas inteligentes y DNI electrónicos para la identificación de usuarios, cada vez aparecen más productos hardware adaptados a esta necesidad, como el teclado con lector de la imagen.

El DNI electrónico

Desde marzo de 2006 es posible obtener una versión electrónica del documento nacional de identidad. Los usos de esta tarjeta van más allá de la simple identificación de personas por parte de autoridades e instituciones físicas. La pretensión es que pueda utilizarse de la misma forma también en Internet, proporcionando acceso a páginas web y servicios institucionales y también a servicios privados como la banca electrónica. Además de los hologramas y otros sistemas de identificación físicos, lo más novedoso es el chip incorporado. En éste se almacena la identidad del propietario del DNI, que mediante un lector especial queda perfectamente identificado de forma electrónica. Además de acreditar la identidad, el DNI electrónico funciona también como firma electrónica. Así, con él podemos grabar nuestra identidad sobre documentos electrónicos, quedando así refrendados por nosotros de la misma forma que si los firmáramos físicamente. Se espera que el DNI electrónico pueda impulsar de forma significativa las medidas de seguridad y acceso, como las que hemos visto en este capítulo, pero también y sobre todo el uso de servicios digitales a través de Internet como la gestión de trámites de todo tipo o el comercio electrónico.



Un aporte extra de seguridad

Accesorios y elementos que convierten nuestro ordenador en un búnker

Más allá de los antivirus y las copias de seguridad, nuestros ordenadores pueden ser protegidos a través de elementos como cámaras, identificadores de huellas digitales o candados y cables de acero para bloquearlos.

1 Bioscrypt VisionAccess 3D DeskCam

Esta cámara para escritorio de ordenador tiene la peculiaridad de funcionar como un sistema de reconocimiento facial en tres dimensiones. Es capaz de distinguir entre 40.000 puntos de identificación en cada rostro y funciona incluso con distintas inclinaciones o posturas. De esta forma, los cambios en nuestro aspecto, como el peinado o incluso el que nos dejemos barba, no suponen ningún problema para que seamos reconocidos correctamente por el sistema. Gracias al software incorporado por la empresa, es posible limitar el acceso a distintos usos del ordenador o directamente al mismo. Es capaz de trabajar con escasa iluminación, ya que las medidas de los parámetros faciales las toma mediante un sensor infrarrojo. El sistema se conecta al puerto USB del ordenador y tiene el aspecto de una simple *webcam* que puede utilizarse tanto en un ordenador de sobremesa como con un equipo portátil. La compañía tiene una gran experiencia en sistemas biométricos por lo que la aplicación de reconocimiento es altamente fiable.

Contacto
Bioscrypt. www.biosciypt.com
,Predo: 250 (aprox.)

2 Dell XPS 1330

Uno de los portátiles más pequeños de la gama Dell nos sirve para mostrar cómo los sistemas de reconocimientos de huellas se han incorporado a la lista de especificaciones de este tipo de ordenadores, y no sólo de esta marca. Este modelo es compacto y ligero, con un peso aproximado de 1,8 kilogramos y una pantalla de 13,3 pulgadas WXGA, por lo que se presta especialmente a que sea sustraído. El sistema de reconocimiento de huellas dactilares que incluye es programable, por lo que se puede configurar para impedir el acceso al ordenador, pero también permite proteger documentos o carpetas importantes, por lo que es posible establecer varios niveles de seguridad sin el engorro de tener que recordar una o varias contraseñas. Dispone de hasta 250 Gbytes de capacidad en el disco duro y procesadores Intel Core 2 Dúo de hasta 2,20 Gigahertzios. Puede adquirirse en dos colores, negro o rojo.

Contacto
Dell, www.dell.es
Precio: QSS'eyrts {aprex,)

3 HTC P6500

Un smartphone basado en Windows Mobile con completas opciones de conectividad inalámbrica gracias a WiFi y Bluetooth, con navegador GPS incorporado y una cámara de tres megapíxeles es, sin ninguna duda, un preciado objeto para ser sustraído. Para evitarlo, así como proteger los datos sensibles que pueda contener, este modelo dispone de un sistema de reconocimiento de huellas dactilares que impide su uso a cualquier persona no autorizada. Se trata de un dispositivo pensado para el entorno empresarial. Dispone de un sistema que permite borrar todos los datos que contiene y las tarjetas que se encuentran conectadas en caso de que el P6500 sea sustraído o extraviado para proteger la información importante que pueda contener. También se habilita un sistema de posicionamiento mediante el GPS incorporado para saber en todo momento dónde se encuentra el terminal. Útil para hacer el seguimiento de una carga o para saber dónde se encuentra el usuario del PDA o el propio dispositivo.

Contacto
HTC. www.europe.htc.com
Precio: 750 euros (aprox.)





4 Kensington PocketSaver

Es posible que, en ocasiones, tengamos que dejar nuestro portátil desatendido para acudir a otro sitio fuera de la oficina o de nuestra casa. En estos casos, los ordenadores se convierten en objeto de un robo. Para no dar facilidades, existen sistemas de seguridad basados en candados y cables de acero que permiten asegurar el equipo a otros objetos, como mesas o barandillas. Existen muchos modelos de distintas marcas especializadas en accesorios para portátiles. En este caso, hemos escogido la propuesta de Kensington, especialmente indicado para que pueda ser llevado cómodamente junto con el portátil. Este elemento dispone de un cable de seguridad enrollable para mejorar su portabilidad. Su peso, tan solo 110 gramos, también contribuye a la comodidad de transporte. Dispone de un sistema de cierre mediante candado con llave y ofrece el sistema patentado de cierre en forma de T para mejorar la seguridad. Un accesorio que nunca está de más si tenemos que usar el portátil en lugares públicos.

Contacto
Kensington, http://es.kensington.com
Precio: 35 euros

5 LaCie d2 SAFE Hard Drive

Todos los dispositivos portátiles presentan la enorme ventaja de que podemos llevarlos con nosotros y utilizarlos en distintas situaciones, pero también tienen la desventaja de que los exponemos a que sean sustraídos o que alguien pueda adquirir los datos que almacenan. En el caso de los discos duros portátiles, estas situaciones también tienen lugar y, por ello, LaCie presenta su gama de dispositivos SAFE, que disponen de un lector de huellas digitales que controla quién utiliza el dispositivo. Pero no sólo se trata del control biométrico, este dispositivo dispone de tres niveles de seguridad para proteger su contenido: el mencionado acceso mediante huella dactilar, cifrado de hardware y cadena de seguridad. El uso del sistema de detección de huellas es sumamente sencillo, basta con apoyar el dedo en el lugar indicado y la unidad se bloquea. Al volver a pasarlo se puede volver a utilizar. Presenta la posibilidad de almacenar hasta cinco usuarios autorizados que podrán bloquear y desbloquear el disco.

Contacto
LaCie. www.lacie.com/es
Precio: 529 euros (1 Terabyte)

6 Microsoft Optical Desktop with Fingerprint Reader

Dentro de la gama de ratones y teclados de Microsoft, existen modelos que incorporan un sistema de lectura de huellas dactilares para añadir de forma más cómoda y eficaz un control de acceso biométrico para nuestro ordenador. En el caso de este modelo, el sensor ha sido colocado en la parte izquierda del teclado. A diferencia de otros sistemas, el de Microsoft ocupa un espacio bastante considerable. El producto se ofrece con el software adecuado para gestionar el uso del lector de huellas. El programa Registration Wizard es el encargado de establecer los niveles de seguridad y clasificar las huellas de los usuarios autorizados, así como de otorgar los permisos pertinentes para los usos de distintos recursos del ordenador. También permite programar el cambio de usuario con sólo apoyar el dedo en el sensor. Microsoft recomienda su uso para aplicaciones como acceder directamente a páginas web que requieran nombre de usuario y contraseña, pero no para entornos empresariales. Es decir, está diseñado más para la comodidad que para el control de acceso.

Contacto
Microsoft, www.microsoft.es
Precio: 115 euros

7 SanDisk Cruzer Profile

Aunque parezca imposible, también se ha conseguido introducir un lector de huellas digitales en una llave de memoria USB. En este caso, se trata de un producto de SanDisk, que ha tenido que aumentar el tamaño de un dispositivo en cualquier caso muy compacto en aras de la seguridad. Mediante este sistema, los datos que contenga la memoria del Cruzer se encuentran a disposición solamente del usuario que se ha registrado como propietario. No es necesario realizar instalaciones de ningún tipo de programa, la información se encuentra protegida en todo momento. Con el producto se entrega una interesante aplicación, el gestor de contraseñas Cruzpass. Mediante éste, el dispositivo USB almacenará todas las claves que utilicemos y podremos acceder a ellas cuando lo conectemos a un ordenador. Así, no tendremos que recordarlas y estarán siempre a mano.

Contacto
SanDisk. http://es.sandisk.com
Precio: 60 euros (1 Gigabyte)

La Red bajo control

La seguridad continúa siendo uno de los grandes problemas en Internet

Los atacantes descubren cada día nuevas formas de rentabilizar sus conocimientos mediante el diseño de nuevas amenazas. Y como sucede con cualquier enemigo, el primer paso es conocer todas sus técnicas v artimañas. Así, con unos sencillos consejos nuestros PC estarán a salvo de las amenazas.

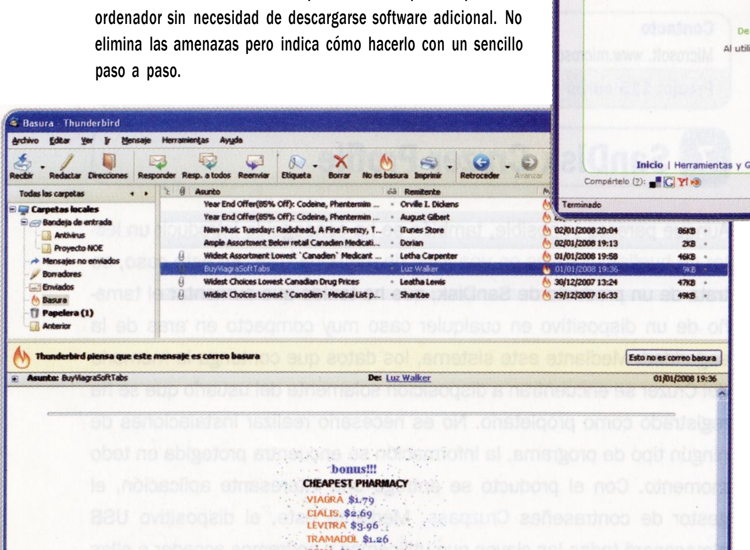
En primer lugar hay que aclarar que aunque los expertos de seguridad han creado distintas categorías para organizar el estudio de las distintas amenazas, las técnicas se entremezclan creando a su vez distintas subcategorias. Sin embargo, al estudiar estas categorías se conocerán las distintas formas que un atacante tiene de infectar un ordenador o robar información personal. En las siguientes páginas repasaremos una a una las principales amenazas de la actualidad y las soluciones más apropiadas para protegerse de cada una de ellas. Hay que advertir de que los diseñadores de *malware* no paran de buscar nuevas técnicas sobre las que apoyarse, por lo que lo que puede valer hoy puede quedarse desfasado en meses, semanas o, incluso, días.

Los virus, la gran amenaza

Desde los principios de la informática personal los virus han sido la mayor amenaza para todos los usuarios de ordenador. Aunque en un principio su expansión era lenta debido a que las infecciones se realizaban a través de soportes magnéticos como los olvidados disquetes, con la llegada de las comunicaciones aumentaron su actividad a casi todos los equipos informáticos. Aunque continúan siendo el principal caballo de batalla para los fabricantes de software de seguridad y existen más de 100.000 versiones distintas, cada vez resulta más complicado que uno de estos virus se extienda por los equipos con cierta facilidad y, en realidad, sólo unas pocas variantes son los responsables del 99% de las infecciones.

Los virus tienen la particularidad de que deben ser ejecutados para dañar un equipo o los datos que contiene. Sus diseñadores aprovechan todo tipo de engaños para obligar al usuario o al sistema a que ejecute el virus. Se apoyan en técnicas como las dobles extensiones o macros contenidas en todo tipo de documentos (DOC, JPG...). Para evitar infecciones hay que ser muy cuidadoso con los programas que se instalan y se ejecutan en un ordenador, pero también con abrir cualquier documento o correo electrónico de procedencia dudosa. En cualquier caso, la única barrera realmente eficaz es un buen programa antivirus.

Desde la web de NanoScan se puede analizar por completo un ordenador sin necesidad de descargarse software adicional. No elimina las amenazas pero indica cómo hacerlo con un sencillo paso a paso.



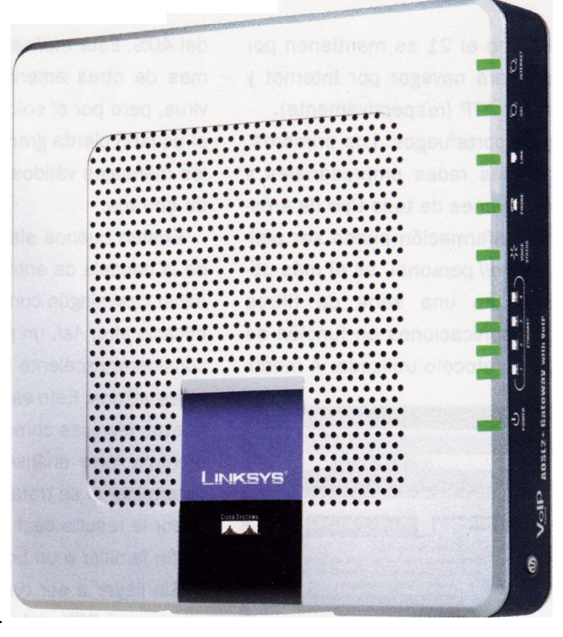
Las actuales técnicas utilizadas para ocultar el *spam* se basan en utilizar documentos de todo tipo para incluir el mensaje publicitario o la amenazada de seguridad. En este caso se utiliza una imagen para dificultar el trabajo al motor *antispam*.

Muchos usuarios consideran que todos los programas son prácticamente iguales. Simplemente esperan a que el software actúe de forma transparente al usuario con la máxima eficacia con sólo instalarlo. Sin embargo, existen grandes diferencias entre productos. Prestigiosos laboratorios especializados en seguridad informática realizan test a los distintos programas de seguridad y ponen sus datos a disposición de todo el público. Por ejemplo, AV Comparatives (www.av-comparatives.org) publica análisis comparativos de los principales programas de seguridad y en sus páginas se puede observar grandes diferencias de seguridad, pero también de rendimiento.

Si los conocimientos de informática del usuario final son escasos, lo más recomendable es recurrir a una *suite* de seguridad que garantice la máxima protección desde el primer momento, como pueda ser el software español Panda Internet Security 2008.

Spyware: infecciones con segunda intención

Mientras que los diseñadores de virus suelen buscar grandes titulares y fama internacional gracias a la «hazaña» de infectar cientos de millones de ordenadores, los delincuentes que dan forma al *spyware* tienen siempre una intención oculta. Puede que quieran utilizar el ordenador infectado para enviar correo basura o quizás busquen información privada o quieran controlar el equipo



Si se activa la seguridad NAT de un *router* se consigue que las direcciones IP de la red interna permanezcan ocultas a un posible atacante.

para realizar ataques masivos a servidores en Internet. Lo que está claro es que el *spyware* está diseñado para quedarse en el equipo, no llamar la atención y realizar su tarea con la mayor eficacia y sigilo. Por esta razón, principalmente, los fabricantes de software de seguridad han decidido crear una aplicación específica para eliminar esta amenaza en lugar de aumentar las funciones del tradicional antivirus.

El *spyware* llega por todo los caminos posibles y aprovecha hasta la mínima vulnerabilidad del sistema para infiltrarse. Si se navega por una página web infectada sin la protección adecuada, si se leen correos basura sospechosos o si se instalan aplicaciones de dudosa procedencia lo más fácil es acabar infectado con alguna de estas amenazas. Pero el *spyware* también puede tomar el control de un ordenador realizando un ataque a las comunicaciones de éste; por tanto, aunque no se realicen acciones arriesgadas las posibilidades de infección siempre son altas. De hecho, se estima que más de la mitad de los ordenadores del mundo son huésped de algún programa *spyware.*

Por todo ello es más que recomendable instalar un software específico para proteger el equipo de estas amenazas, normalmente integrado en una *suite* más completa. Pero si se tiene la sospecha de que el equipo está infectado (procesos en el sistema desconocidos, equipo ralentizado...) se pueden recurrir a un análisis de *spyware* basado en web. Eso sí, ojo porque muchas páginas que ofrecen este servicio no son más que una tapadera para infectar más, por lo que hay que elegir siempre fabricantes con cierto prestigio.

Algunas *suites* de seguridad como Norton Internet Security 2008 ofrecen una excelente calificación en las pruebas del laboratorio AV Comparatives.

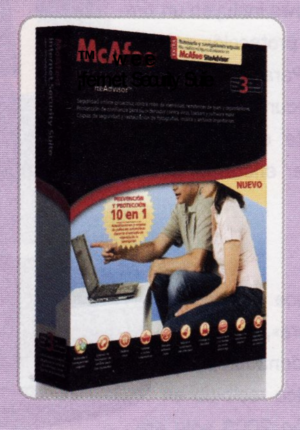
Actualmente el análisis basado en web más popular es NanoScan (www.nanoscan.com), de los ya mencionados Panda Software. Su funcionamiento es muy sencillo: basta descargar un pequeño control ActiveX o un *plug-in* (depende de si utilizas Internet Explorer o Firefox) y el sitio web te guía a través de todo el proceso de análisis del sistema. Si el ordenador está infectado con alguna de las más de dos millones y medio de amenazas, este pequeño programa lo detectará. Sin embargo, NanoScan no elimina las amenazas, sólo las detecta por lo que habrá que registrarse en Panda para utilizar su programa TotalScan. El registro es gratuito y ofrece una solución de garantías para librarse del *spyware,* aunque no es una solución de seguridad efectiva a largo plazo.

Cortafuegos, la primera barrera

Todo el mundo tiene claro que debe proteger su ordenador frente a los virus con un buen programa antivirus, pero muy pocos saben que un cortafuegos, o *firewall,* es imprescindible para completar la seguridad de cualquier equipo. Los cortafuegos simplemente definen normas de seguridad para impedir que posibles intrusos tengan acceso al equipo a través de las comunicaciones. Simplemente, mientras que un antivirus o *antispyware* detecta y elimina las amenazas, el *firewall* reduce al mínimo las posibilidades de infección. Su función principal es la de proteger las comunicaciones. Para conseguirlo, bloquea todos los puertos que no se utilizan normalmente y los oculta para que no estén siquiera al alcance de

Qué hacen nuestros hijos cuando navegan por la Red

Para casi cualquier niño la palabra «prohibido» resulta más tentadora que cualquier contenido de Internet por lo que, en la mayoría de los casos, prohibir a tu hijo navegar por páginas web de contenido violento o pornográfico puede resultar una tarea inútil. Además, la supervisión continua por parte de un adulto parece una tarea imposible, ya que pueden tener ordenador en su habitación, o un portátil con conexión WiFi, o llegar a casa antes de que lo hagan los padres... Por lo tanto, una solución puede ser utilizar uno de los programas que proporcionan control sobre el tipo de páginas web que se pueden visitar. Tras asociar una de estas aplicaciones a un perfil de usuario, se puede determinar el nivel de seguridad para restringir el acceso a determinados contenidos e incluso limitar el tiempo de uso y los horarios aceptables. Estas aplicaciones basan su funcionamiento en dos tipos de bases de datos. La primera contiene todas las palabras o frases que se quieren censurar. Así, si por ejemplo el niño quiere acceder a un contenido sexual identificará palabras claves de la web como «sexo» o «tetas» y bloqueará la página. La segunda determina directamente las páginas web que contienen estos contenidos. Esta base de datos se actualiza periódicamente desde el servidor del proveedor de software de modo que bloquea gran cantidad de páginas antes incluso de descargarlas.

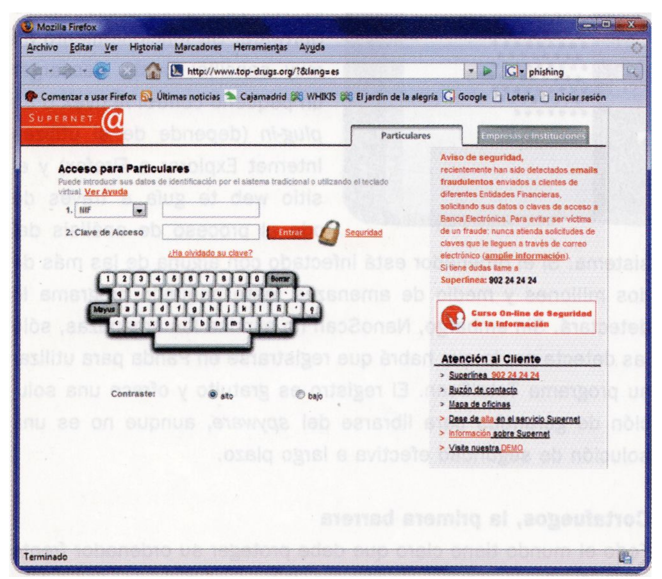


El control parental permite gestionar el número de horas que los más pequeños pasan en Internet. Este es el caso de la *suite* de seguridad de McAfee.

posibles ataques. Algunos como el 80 o el 21 se mantienen por defecto abiertos, ya que se utilizan para navegar por Internet y para realizar transferencias de archivos FTP (respectivamente).

Existen dos tipos fundamentales de cortafuegos. Los primeros, servidores *proxy,* se utilizan en grandes redes empresariales y analizan todo el tráfico en busca de patrones de todo tipo de amenazas. Así, este software decide qué información puede ser peligrosa y la bloquea. El otro tipo, el *firewall* personal, es el más utilizado. Su funcionamiento se basa en una serie de filtros diseñados para analizar todas las comunicaciones en función de la fuente, los puertos de destino y el protocolo utilizado. A menudo estos filtros están presentes en los *routers* que se utilizan para crear las pequeñas redes o acceder a Internet y se conocen como Seguridad NAT. Puede resultar complicado para algunos usuarios domésticos definir las reglas de seguridad de su *router,* pero merece la pena el esfuerzo, ya que de este modo ocultará a posibles atacantes la dirección IP de cada uno de los ordenadores conectado al router.

Los cortafuegos personales basados exclusivamente en software no son capaces de ocultar las direcciones IP de manera eficaz, pero sí de analizar toda la información enviada o recibida en el ordenador y bloquear la mayoría de las amenazas de seguridad antes de que se internen en el equipo. Las últimas versiones de Windows incluyen un *firewall* personal que ofrecen un nivel de protección mínimo contra los ataques más habituales. Para conseguir un nivel de seguridad alto es necesario recurrir a productos especializados y leer cuidadosamente el manual de usuario para ser capaces de configurar eficazmente el programa.



Aunque pueda parecer que la página web es totalmente legal e idéntica a la original, en realidad se trata de un fraude diseñado para captar los datos de acceso de las víctimas mediante técnicas de *phishing.*

El reinado del correo basura

El *spam,* nombre con el que se conoce a todos los correos no solicitados, o «correo basura», se ha convertido en la principal plaga de un ordenador personal. Sobre el 95% del correo electrónico recibido en una cuenta es spam, cuando en el año 2003 sólo era del 40%. Este *malware* está pensado para la infiltración en los sistemas de otras amenazas como puede ser todo tipo de *spyware* y virus, pero por sí solo supone un grave problema ya que provoca que el usuario pierda gran cantidad de tiempo mientras intenta identificar los mensajes válidos dentro de su normalmente abarrotada bandeja de entrada.

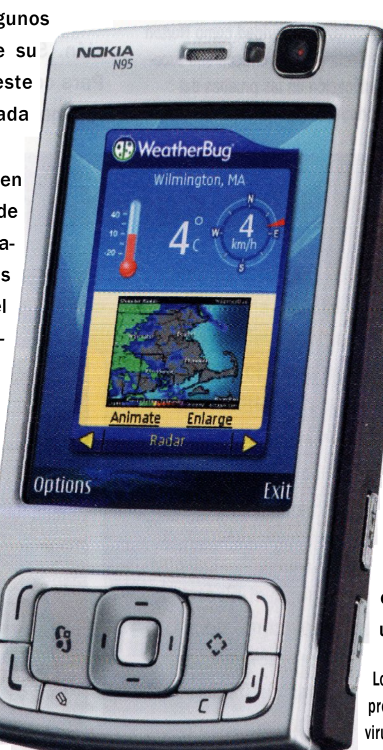
Existen buenos sistemas *antispam* capaces de mantener alejados de la bandeja de entrada la mayor parte de los correos basura sin eliminar casi ningún correo real. Sin embargo, aún no tienen un índice de eficacia alto. Así, un programa que elimine el 80% del *spam* se puede considerar excelente siempre que apenas descarte un 3% de los mensajes válidos. Esto es debido a que el *spam* no para de evolucionar con nuevas técnicas como la utilización de imágenes, audio y todo tipo de archivos cuyo análisis informático resulta muy complejo como para determinar si se trata o no de correo deseado. Por ejemplo, a un ordenador le resulta casi imposible determinar si una imagen es una fotografía familiar o un bote de las famosas pildoras azules.

Sin llegar a ser demasiado catastrofistas, hay que reconocer que eliminar el 80% del *spam* facilita la lectura del correo. Por lo tanto, si se utiliza algún programa de lectura de correo como Outlook o Eudora es casi obligatorio recurrir a un programa *antispam.* De hecho, la mayoría de éstos ya disponen de su propio sistema de protección, pero si no se está contento con los resultados se puede recurrir a aplicaciones de terceros fabricantes. Todas las empresas de software de seguridad tienen diseñados sistemas de este tipo, aunque rara vez se venden como un producto aislado ya que suelen incluirse en *suites* de seguridad junto a antivirus, *firewall* y demás soluciones software. También se puede encontrar algunas aplicaciones gratuitas que realizan esta tarea, como SpamExperts (www.spamexperts.com), pero su eficacia y, sobre todo, su manejo no están a la altura de soluciones más profesionales como las proporcionadas en las mejores *suites* de seguridad.

Phishing: estafa a domicilio

Una de las mayores amenazas actuales en Internet es el *phishing.* Esta práctica consiste en el envío de correos electrónicos a víctimas potenciales suplantando la identidad de su banco, su proveedor de Internet o un establecimiento comercial con el objetivo de conseguir información personal del destinatario. Por supuesto, estos datos son utilizados posteriormente para realizar estafas como la extracción de dinero de las cuentas bancarias o la compra de todo tipo de productos con cargo a los incautos estafados.

El cebo es el correo que imita a la perfección el estilo de la entidad suplantada e incita a conectarse a una página web a través de un enlace contenido en el cuerpo del mensaje. Sin embargo, el enlace es falso y dirige al usuario en cuestión a una copia fraudu-



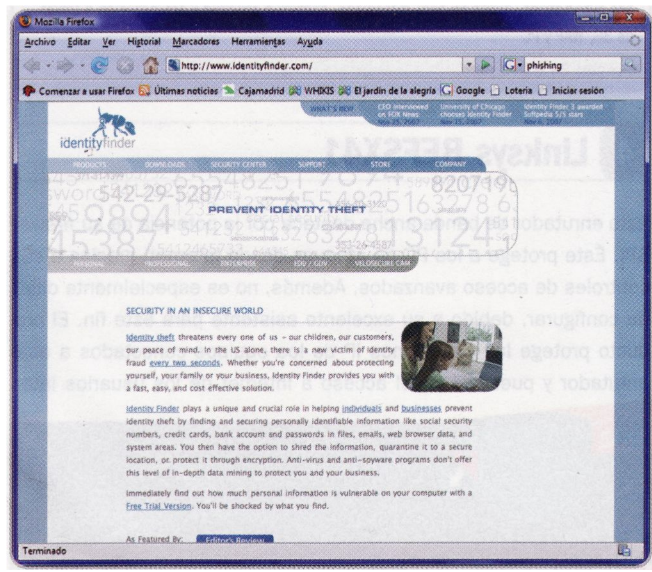
Los terminales con sistema operativo como el Nokia N95 proporcionan una plataforma para el ataque de nuevos virus y otro malware. Por suerte, empresas como Symantec ya han diseñado antivirus para estos teléfonos.

Rootkit de derechos de autor

Aunque aún no sean todo lo populares que deberían, hay que decir que los *rootkits* son un tipo de troyano que se mantiene oculto frente a detecciones y, a su vez, oculta otros archivos, entradas de registro o conexiones de red. Este tipo de aplicaciones permite al atacante tener acceso completo al ordenador, lo cual significa que puede manejar el equipo a su antojo. Es capaz de bloquear las peticiones de visualización de un archivo por parte de cualquier programa o incluso proporcionar datos incorrectos al sistema. Por otro lado, estos *rootkits* se están utilizando actualmente para otros propósitos que algunos vendedores consideran totalmente legítimos. Por ejemplo, si se instala software compatible con DRM (gestión de derechos digitales) y se mantiene oculto, puede controlar el uso de programas bajo licencia o contenidos protegidos bajo *copyright*. Sin embargo, este software DRM se protege a sí mismo frente a una desinstalación y, en el fondo, no es mejor visto que un *spyware* que ataca al sistema y utiliza técnicas de *rootkits* para ocultarse frente a análisis.

lenta de la web de la entidad de la que los estafadores obtendrán los datos personales, lo que les permitirá suplantar la personalidad del estafado. En realidad, el cebo se envía de manera masiva con la esperanza de que un mínimo porcentaje de usuarios caigan en la trampa. Un índice de éxito de menos del 0,5% puede proporcionar información suficiente para conseguir una importante suma de dinero.

Existe una variante más personal y dirigida, en la que el atacante manda mensajes de correo a un grupo definido de personas suplantando la personalidad de un individuo importante de su organización, como el responsable de recursos humanos o el

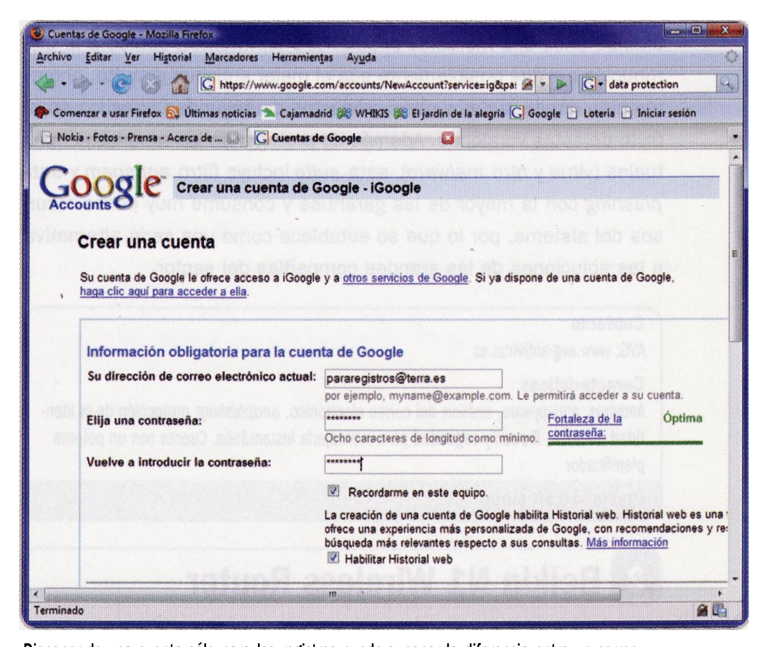


En la web www.identityfinder.com podremos asegurar toda la información personal y gestionarla de manera que la habitualmente tediosa tarea de rellenar formularios sea más sencilla y segura a la vez.

administrador de su red. Si alguno de los receptores del mensaje cae en el engaño, el atacante puede conseguir un mayor acceso dentro de la organización o directamente información privada potencialmente valiosa. La mayoría de las *suites* de seguridad incluyen una aplicación especializada en bloquear estas amenazas. Su funcionamiento se basa en avisar al usuario del acceso a páginas web sin certificado de seguridad válido y en contar con una base de datos con todas las páginas detectadas como fraudulentas. Sólo así se consigue el máximo de protección ante esta peligrosísima amenaza.

Datos personales protegidos

Mientras que en nuestra vida real somos muy celosos de nuestra identidad y no proporcionamos nuestros datos privados a la primera persona que los pregunta, en Internet sí solemos rellenar cientos de formularios con todo tipo de información de carácter privado. Es de vital importancia proteger estos datos y ponerlos a disposición solamente de aquellos que conozcamos personalmente o con los que queramos iniciar una relación empresarial. En primer lugar, al rellenar un formulario lo recomendable es rellenar sólo los cuadros que sean imprescindibles y siempre asegurarse de que las casillas de verificación relacionadas con la distribución de los datos están siempre activadas para que la empresa receptora no pueda distribuirlos en función de sus intereses. En nuestro país estas casillas deben estar activadas por defecto, pero en otros países la normativa es diferente. Hay que tener en cuenta que aunque la página parezca realizada en España en realidad podría estar alojada en cualquier otro lugar.



Disponer de una cuenta sólo para los registros puede suponer la diferencia entre un correo repleto de *spam* y otro prácticamente a salvo.

Algunas páginas requieren registrarse para acceder a contenidos adicionales. Si no hay un especial interés por mantener una relación duradera con estas web lo más lógico es mentir. También es recomendable crear una cuenta de correo «paralela» para utilizarla en estos casos, ya que normalmente la activación del registro se realiza a través de mail. Por otro lado, hay que evitar cuentas de los principales proveedores de correo web (como Hotmail), ya que muchas páginas de registro rechazan estas direcciones. Algunos programas del mercado están especializados en proteger la información personal. Por ejemplo, IdentityFinder (www.identityfinder.com) asegura toda la información personal y la gestiona de modo que tareas como rellenar formularios resultan más sencillas y, sobre todo, más seguras.

Máxima protección

Una muestra del software y el hardware idóneo para blindar tu equipo

Algunas herramientas nos pueden ayudar a conseguir un equipo fuerte frente a las numerosas amenazas e intrusiones que puede sufrir. Veamos algunas de las propuestas que están disponibles en el mercado.

1 AVG Internet Security 7.5

Esta compañía de seguridad informática ha conseguido durante los últimos años una merecida popularidad en Internet, debido a la distribución del que posiblemente sea el mejor antivirus gratuito. Ahora, también ofrece *suites* y otros productos de seguridad basados en el éxito de estas versiones. Además de proteger de las amenazas habituales (virus y otro *malware*), esta *suite* incluye filtro *antispam* y *antiphishing* con la mayor de las garantías y consume muy pocos recursos del sistema, por lo que se establece como una seria alternativa a las soluciones de las grandes compañías del sector.

Contacto
AVG. www.avg-antivirus.es
Características
Antivirus, antispyware, análisis del correo electrónico, *antiphishing,* protección de la identidad en línea, *firewally* seguridad para mensajería instantánea. Cuenta con un potente planificador
Precio: 46,90 euros

2 Belkin NI Wireless Router

Este módem ADSL con *router* inalámbrico destaca por ofrecer una excelente calidad de transmisión y cumplir con los estándares actuales de seguridad WPA y WPA2. Además de proteger la conexión frente a posibles *hackers,* es posible distribuir vídeo en alta definición, gracias a los 300 Mbps de tasa de transmisión. A su impecable diseño se une una serie de indicadores que permiten a cualquier usuario determinar el estado de la red sin necesidad de tener conocimientos avanzados. Además, pronto estará disponible la actualización de su *firmware* para adaptarse al estándar 802.lln.

Contacto
Belkin. www.belkin.es
Características
Transmisión hasta 300 Mbps. Alcance hasta 420 metros. Estándares soportados: IEE 802.11b, 802.llg y 802.11n (borrador). Dimensiones: 156 x 40 x 174 mm. Peso: 300 gramos. Soporta WPA y WPA2
Precio: 159 euros

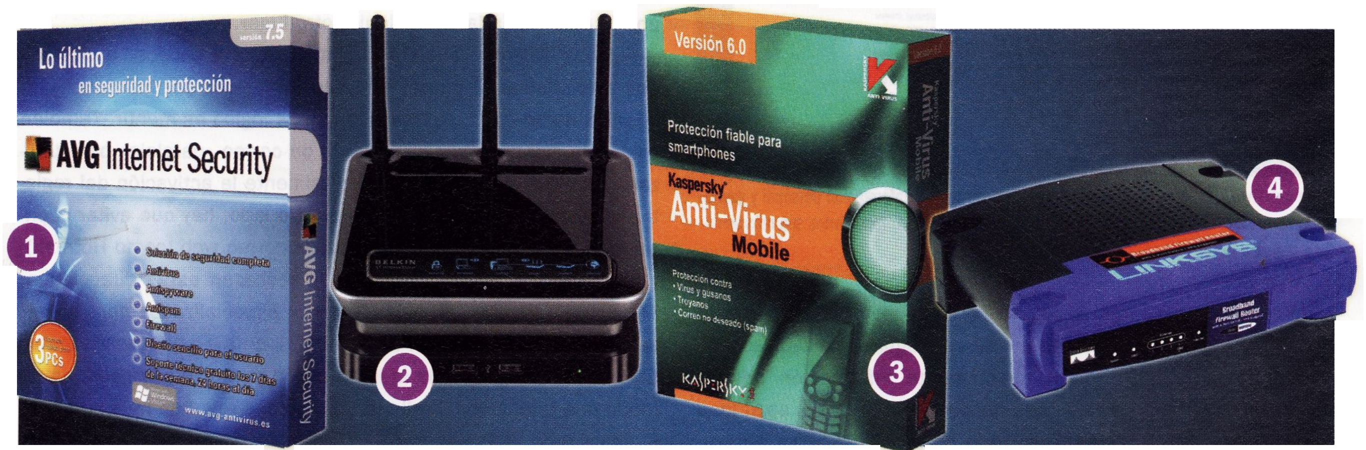
3 Kaspersky Anti-Virus Mobile

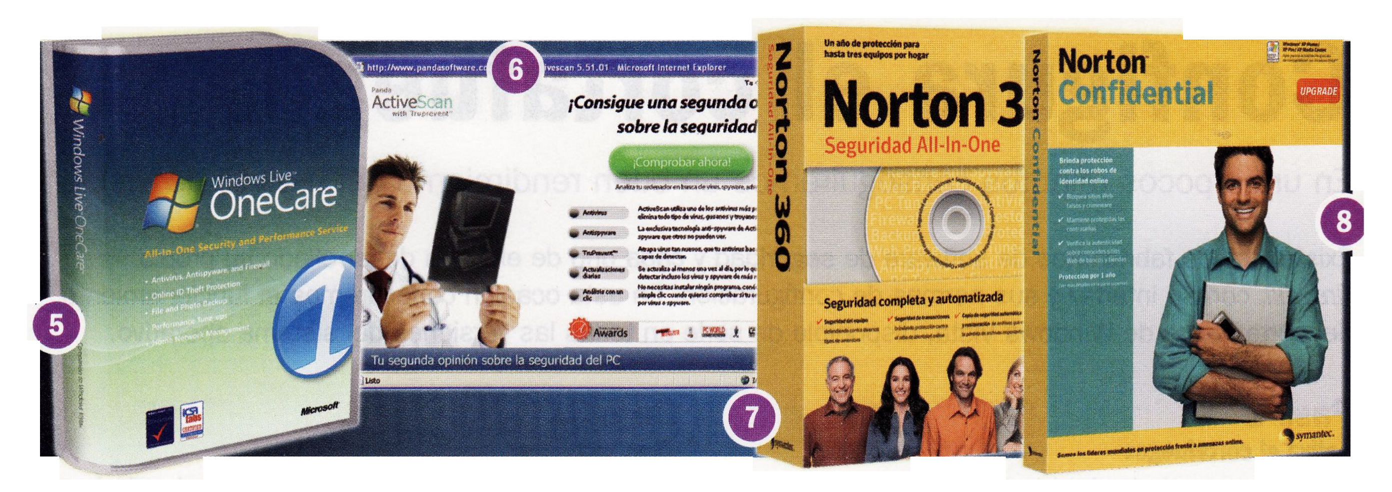
Del mismo modo que los teléfonos inteligentes (*smartphones*) actuales son capaces de ejecutar todo tipo de aplicaciones, también se han convertido en un caldo de cultivo ideal para la proliferación de virus y todo tipo de *malware.* No se trata de una amenaza a medio o largo plazo, ya hay circulando algunas versiones capaces de atacar algunos de los sistemas operativos más utilizados en estos dispositivos. Kaspersky se ha adelantado y antes de que esta amenaza se convierta en una plaga ha lanzado una propia versión de antivirus para terminales móviles. Por ahora, hay versiones para Symbiam OS y Windows Mobile.

Contacto
Kaspersky. www.kaspersky.es
Características
Antivirus, *antispyware,* análisis del correo electrónico, análisis programado, actualizaciones automáticas, *antispam* para mensajería, análisis a solicitud y actualización a través de 3G, WAP y PC
Precio: 29,95 euros

4 Linksys BEFSX41

Este enrutador de banda ancha destaca por la potencia de su *firewall* SPI. Éste protege a los PC de ataques desde Internet, gracias a sus controles de acceso avanzados. Además, no es especialmente difícil de configurar, debido a su excelente asistente para este fin. El producto protege las direcciones IP de los equipos conectados a este enrutador y puede filtrar el acceso a Internet de los usuarios inter-





nos. También permite denegar el acceso a equipos ajenos, gracias a sus sistemas de protección por direcciones MAC.

Contacto
Linksys. www.linksys.es
Características
Soporta hasta dos redes privadas virtuales, protección frente al ping de la muerte, denegación de servicio, ataque terrestre, IP *spoofing*y otros ataques DoS. Soporta SNMP 2, IEE 802.3 y 802.3u. Dimensiones: 186 x 48 x 154 mm. Peso: 380 gramos
Precio: 64 euros

5 Microsoft Windows Live OneCare

Todas las *suites* de seguridad se integran con el sistema operativo. Algunas consiguen que la compenetración con el mismo sea máxima, pero otras pueden incluso crear graves problemas de compatibilidad. Para evitar estos riesgos, la opción más acertada es Windows Live OneCare. Este servicio de Microsoft se integra a la perfección con todos los sistemas Windows actuales, como no podía ser de otra manera. El nivel de protección que ofrece no es especialmente alto, pero, para todo aquel que esté acostumbrado a utilizar las aplicaciones de esta firma, resultará realmente intuitivo.

Contacto
Microsoft, http://onecare.live.com
Características
Antivirus, antispyware, análisis del correo electrónico, *antiphishing*, ajuste del sistema, protección del *firewall*, copia de respaldo y restauración automáticas e integración en Messenger
Precio: 49,95 euros

6 Panda ActiveScan Pro

En páginas anteriores hablábamos sobre las bondades del análisis de virus y otras amenazas *on-line*. Panda ha desarrollado herramientas muy potentes en este campo y ofrece una versión avanzada de su análisis en línea: Panda ActiveScan Pro. Por un módico pago anual, protege cualquier equipo de más de 110.000 virus y otro *malware*. No ofrece otras funciones de seguridad como *firewall* o *antispam*, ni siquiera protege en tiempo real, pero tampoco acapara el sistema y consume todos los recursos. Recordamos que se puede probar este servicio antes de utilizarlo desde la página web del fabricante.

Contacto
Panda, www.pandasecurity.es
Características
Análisis y desinfección de virus, análisis y desinfección de *spyware*, análisis y desinfección de otro *malware*, más de 110.000 definiciones de virus, compatible con Internet Explorer (ActiveX) y con Firefox 2.0 (*add-on*). Realiza detección heurística
Precio: 19,95 euros

7 Symantec Norton 360

Aquellas personas especialmente interesadas en la seguridad suelen confeccionar su propio sistema aunando las características de varios productos que, en ocasiones, suelen ser de fabricantes de software diferentes. Para todos los demás lo más útil es un paquete que integre todos los programas necesarios. Este es el caso de Norton 360. Además, es la *suite* que ofrece mejor protección desde el primer momento, ya que su configuración por defecto es muy efectiva. Productos similares de otras compañías (como Kaspersky) necesitan decenas de configuraciones antes de ofrecer una protección completa.

Contacto
Symantec, www.symantec.es
Características
Suite que incluye antivirus, *antispyware*, análisis del correo electrónico, *antiphishing*, protección de la identidad en línea y *firewall*. Realiza copias de respaldo y restauración automáticas. 2 Gbytes de almacenamiento en línea
Precio: 89,99 euros

8 Symantec Norton Confidential

Debido a la gran cantidad de *spyware* que circula por Internet es muy recomendable utilizar un programa de protección de la identidad, sobre todo si se realizan compras. Esta aplicación cifra y protege todas las contraseñas utilizadas en el sistema con especial atención a los datos bancarios que se han facilitado durante las compras. Además, identifica todo tipo de sitios web sospechosos comprobando los certificados y cotejándolos con sus propias bases de datos. También bloquea los programas de registro de pulsaciones de teclado y las capturas de pantalla para evitar que los *keyloogers* consigan realizar su trabajo.

Contacto
Symantec, www.symantec.es
Características
Protege tu identidad, detecta los sitios web sospechosos, verifica y autentica los sitios web válidos, intercepta el correo electrónico de *phishing*, bloquea los programas de registro de pulsaciones de teclado y las capturas de pantalla, y cifra y protege las contraseñas
Precio: 37,49 euros

Configura el cortafuegos

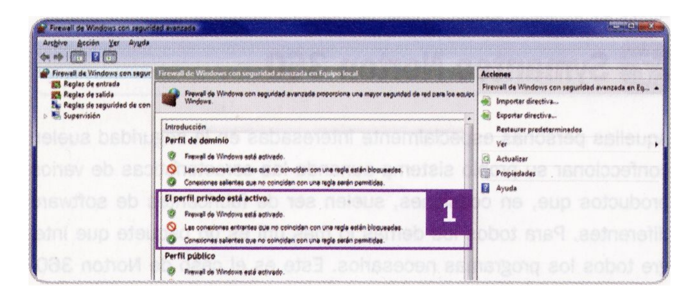
En unos pocos minutos conseguiremos un buen rendimiento del firewali de Vista

Existen varios fabricantes de software de seguridad y cada uno de ellos ha desarrollado su propio *firewali,* con su interfaz y sus normas de configuración. En esta ocasión conoceremos el funcionamiento del cortafuegos de Windows Vista, disponible de serie en todas las versiones del sistema operativo.

Paso 1

Activa el cortafuegos

Con la nueva consola de administración del *firewali* se pueden crear reglas más complejas que con la versión para XP. Éstas se pueden aplicar tanto a la entrada como a la salida de datos y soportan un nivel de configuración muy avanzado para tratarse de software no especializado.

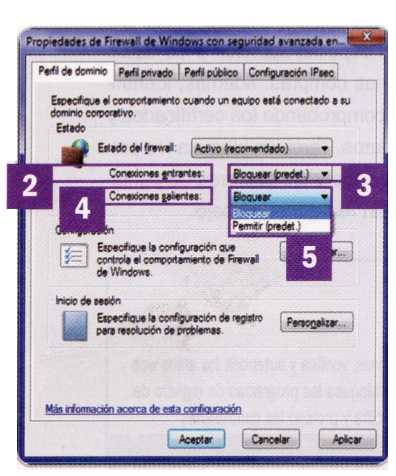


En primer lugar, hay que acceder a la consola Firewali de Windows. La manera más sencilla es escribir WF.msc en el buscador de Vista (dentro del menú de Inicio). Como se puede ver en este momento, el estilo de la consola es MMC 3.0, por lo que los administradores estarán familiarizados con este tipo de entornos. En cualquier caso, para acceder a las propiedades del *firewali,* basta con mostrar las Propiedades de la entrada Firewali de Windows... situada en la parte izquierda de la ventana (con el botón derecho). En este punto, y siempre que el ordenador sea de uso personal, hay que seleccionar la pestaña Perfil privado. En este momento, sólo hay que asegurarse de que el Estado del cortafuegos sea Activo [i],

Paso 2

Bloquea las conexiones

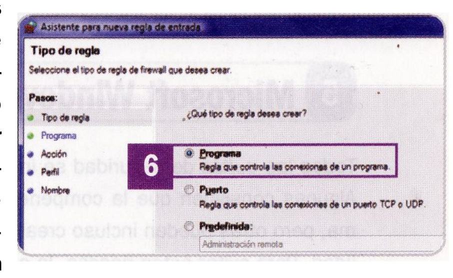
El *firewali* de Vista siempre fija el valor de Conexiones entrantes [2] como Bloquear (predet.) [3], esto significa que bloquea toda información que llega al equipo a no ser que cumpla una serie de reglas predeterminadas. Por su parte, el valor del campo Conexiones salientes [4] es de Permitir (predet) [5], lo que indica que permite el envío de todo tipo de información. Si se cambia esta opción por Bloquear, el nivel de seguridad aumenta, ya que también bloqueará posible información confidencial enviada desde el equipo hasta un servidor remoto por una posible muestra de *malware (spyware, keylooger...).* Por último, basta con pulsar el botón Aceptar para aplicar los cambios.



Paso 3

Crea una nueva regla

Como sucede en todos los cortafuegos, son una serie de reglas las que determinan su comportamiento. En Vista, los usuarios pueden crear las suyas propias o personalizarlas en función de sus necesidades. Para ello, desde la ventana de Firewali de Windows, basta con seleccionar Reglas de entrada (situada en la parte izquierda) y, posteriormente, en el enlace Nueva regia (situada en la parte derecha) para iniciar el asistente. En este caso, crearemos una para permitir las comunicaciones al navegador. Esto se consigue seleccionando la opción Programa [6] de la lista de opciones y pulsando el botón Siguiente. En la siguiente pantalla del asistente, tendremos que decidir de qué modo se aplica esta regla o a qué programa. Como en este ejemplo sólo buscamos permitir al navegador acceder a Internet, seleccionaremos la opción Esta ruta de acceso del programa, pulsaremos Examinar y buscaremos en el explorador el ejecutable del navegador, en este caso firefox.exe. Por último, hay que pulsar el botón Siguiente de nuevo.

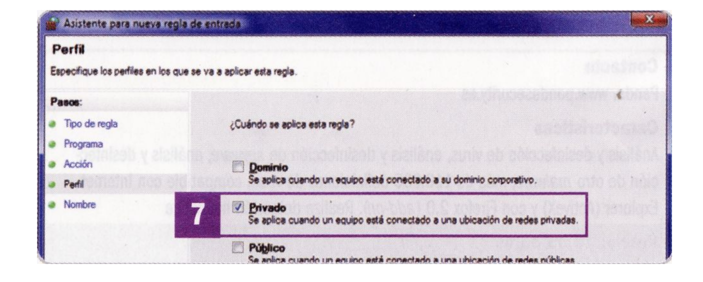


Paso 4

Define las reglas

En la siguiente pantalla del asistente de configuración, hay que definir la medida que debe tomar el *firewali* en función del tipo de conexión (entrante en este caso). La opción Permitir la conexión, si es segura, asegura la identidad del emisor, por lo que ofrece un nivel de seguridad superior (para redes configuradas con IPSEC), pero, por el contrario, puede que muchas de las conexiones no se puedan completar. En este caso, marcaremos Permitir la conexión y pulsaremos el botón Siguiente.

La siguiente ventana nos pregunta sobre el ámbito de aplicación de la regla. En este caso, como es un ordenador de uso personal, la opción correcta es Privado [7]. En el último paso, sólo hay que introducir un Nombre para la regla, una corta Descripción y pulsar el botón Finalizar. De este modo, si se crean reglas de entrada y/o salida para cada programa utilizado, se aumenta la seguridad del equipo sin necesidad de recurrir a software de terceros.



Seguridad NAT con un router

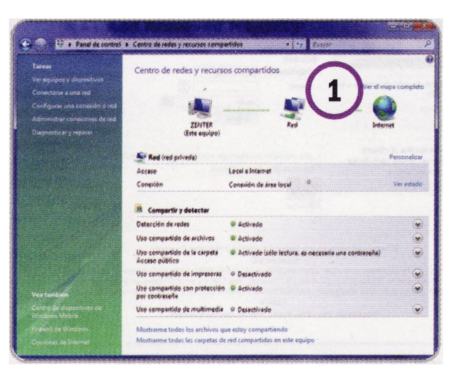
Te enseñamos a configurar la primera barrera de seguridad de cualquier equipo

Si consideramos el sistema de seguridad como una cebolla compuesta por capas, el *router* sería la primera barrera de protección. En unos pocos pasos puede ser el mayor aliado de un *firewall* basado en software y un buen sistema antivirus.

Paso 1

Determina la puerta de enlace

En las configuraciones de red caseras que utilizan un *router,* la dirección de este dispositivo suele dar acceso a la interfaz de configuración web. Esta dirección coincide en casi todos los casos con la puerta de enlace de todos los elementos de la red, por lo que se puede averiguar sin ningún problema. Para ello, hay que abrir, en el Panel de Control, el Centro de redes y recursos compartidos (Windows Vista) [1] y pulsar sobre el enlace Ver estado de la conexión. A continuación, pulsaremos sobre el botón Detalles y apuntaremos tanto la IPv4 Dirección IP como IPv4 Puerta de enlace predeterminada. Con estos dos datos ya se puede acceder a la configuración web de la seguridad NAT de prácticamente cualquier *router.*

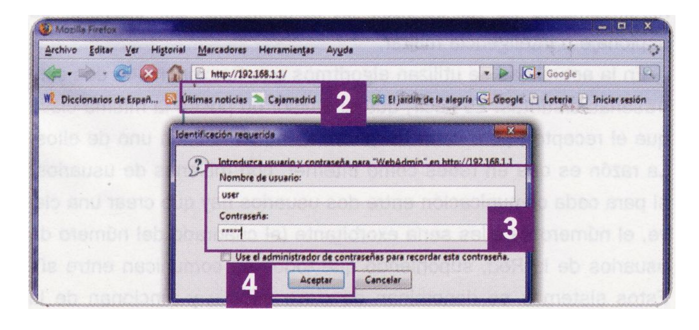


Paso 2

Acceso a la configuración web

Los módems-routers distribuidos por los principales ISP (Proveedores de Servicios de Internet, por ejemplo Telefónica) cuentan con un modo de configuración a través de web. Las opciones pueden estar más o menos bloqueadas en función de los intereses comerciales de los propios ISP y de la versión del propio dispositivo, pero casi todos cuentan con un apartado que permite administrar la seguridad NAT.

Para acceder a esta interfaz de configuración, basta con abrir un navegador (Internet Explorer, Firefox...) e introducir en la barra de direcciones la IP correspondiente a la puerta de enlace obtenida en el paso anterior [2]. Tras realizar esta acción, aparecerá una ventana de autenticación en la que habrá que introducir el nombre de usuario y la clave correspondiente [3]. Estos datos los puede proporcionar el ISP y, seguramente, aparezca en el manual de servicio correspondiente a la conexión o al dispositivo. Después, sólo resta pulsar el botón Aceptar [4] para entrar en la interfaz.

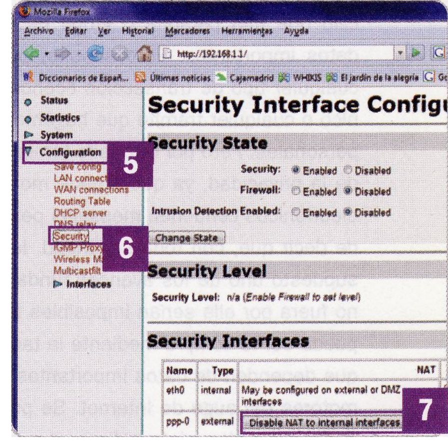


Paso 3

Activa la seguridad NAT

Cada *router* es distinto, por lo que no se pueden definir una serie de pasos que funcionen con todos los dispositivos. Sin embargo, como el objetivo es el mismo, unas pequeñas directivas y consejos facilitarán encontrar los pasos a seguir.

El primer paso consiste en encontrar una pestaña u opción de configuración. En este momento, las estadísticas y otros informes no son de gran utilidad. En segundo lugar, hay que encontrar la opción relacionada con seguridad NAT (casi siempre se encuentra bajo funciones Security, NAT, Interfaces NAT o similares). Tras seleccionarlas, hay que buscar las interfaces y activar la seguridad NAT para la interna.



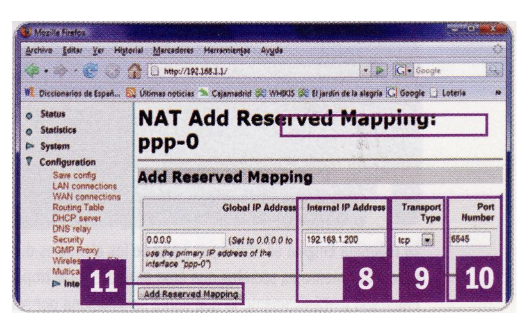
Por ejemplo, con un *router XaV* de Amper los pasos son los siguientes: desplegar los menús Configuration [5] y Security [6] y pulsar el botón Enable NATto internal interfaces [7] para activar la seguridad NAT.

Paso 4

Crea una regla NAT

Al activar la seguridad NAT, los puertos de comunicaciones utilizados por algunos programas se pueden bloquear. Para evitarlo, hay que proceder a reservar puertos en la interfaz de configuración NAT. Antes de empezar, hay que conocer los puertos y protocolos que utiliza el programa bloqueado así como la dirección IP del PC que ejecuta la aplicación.

Este proceso es un poco más complejo. A modo de ejemplo, en el *router* que hemos utilizado para este caso práctico, los pasos a seguir son los siguientes. En primer lugar, hay que hacer clic sobre el enlace Advance NAT Configuration para iniciar la configuración de los puertos. Después, hay que pulsar sobre Add Reserved Mapping y rellenar los campos Internal IP Address [8] (con la IP del ordenador), Transport Type [9] (tipo de protocolo; TCP, UDP ...) y Port Number [10] (el número del puerto). Por último, basta con pulsar el botón Add Reserved Mapping [11] para establecer una nueva reserva o, coloquialmente, abrir un puerto.

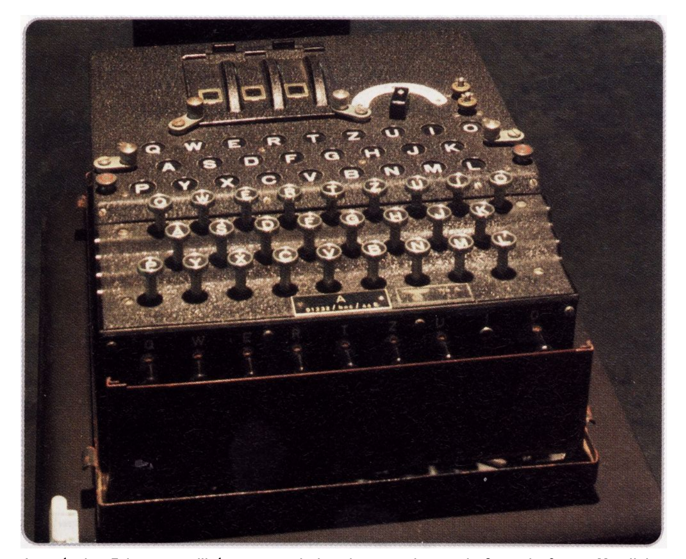


El encanto del anonimato

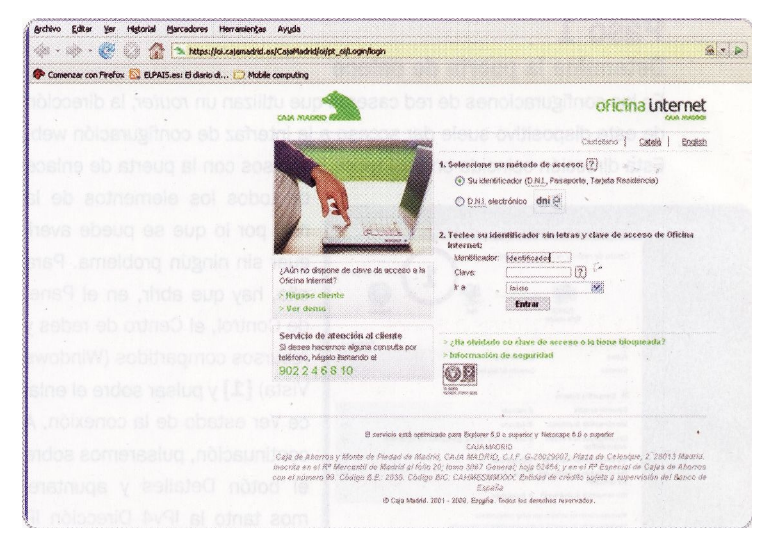
En busca de la seguridad total en el intercambio de datóos a través de -Internet

Por la Red viajan millones de bytes en forma de datos importantes como cuentas bancarias, números de tarjetas de crédito, historiales médicos... pero también mensajes privados que no nos gustaría que pudieran leer otras personas.

Para proteger estos datos se utiliza una práctica que tiene muchos años de antigüedad (de hecho es muy anterior a la existencia de Internet) y gracias a cuya aplicación podemos estar razonablemente protegidos. Estamos hablando de la criptografía. Y es que, tal y como está diseñada la Red, es relativamente sencillo que una persona o grupo de personas consiga hacerse con datos importantes. Esto supone, por un lado, una amenaza ante cualquier tipo de transacción económica, como el comercio electrónico o cualquier trámite que hagamos por Internet manejando datos personales. Pero por otro lado también supone una posible violación de la privacidad, ya que a cada momento miles y miles de correos electrónicos contienen mensajes personales. Por esta razón se puede decir que, con toda seguridad, la criptografía y su aplicación ha supuesto uno de los avances fundamentales dentro de Internet. Si no fuera por ella serían imposibles las transacciones seguras como pueda ser la compra mediante la tarjeta de crédito y otros procesos que dependen de datos importantes y que han supuesto uno de los motores del auge de Internet. Se puede decir que sin la aplicación de los principios criptográficos no existiría el comercio electrónico. La criptografía, además, pone a nuestra disposición los instrumentos para convertir en completamente privados nuestros mensajes de correo electrónico consiguiendo que éstos lleguen sólo a su destinatario. Es un proceso menos utilizado pero igualmente valioso y que en muchos países supone mucho más de lo que podemos imaginar. En cualquier caso, nunca está de más proteger nuestra privacidad, y más adelante veremos cómo conseguirlo. La criptografía también facilita otras aplicaciones como la firma digital, que no es más que un código único y oculto que identifica a una persona para que quien reciba un mensaje pueda estar seguro de su origen. Además, también sirve para rubricar documentos electrónicos.



La máquina Enigma se utilizó por parte de los alemanes durante la Segunda Guerra Mundial para cifrar mensajes secretos que eran enviados a las tropas y a los servicios de inteligencia. Realizaba mecánicamente lo que ahora se soluciona por software de forma casi instantánea.



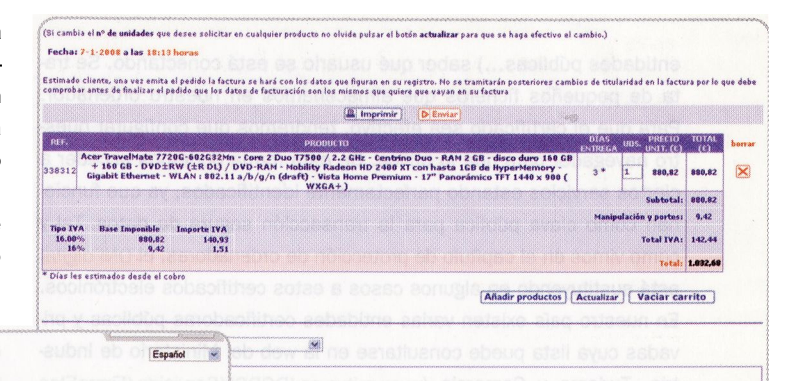
Algunas páginas web, como las oficinas virtuales de los bancos, disponen de un sistema de conexión segura para garantizar que los datos que se están proporcionando no son interceptados por otros que puedan utilizarlos para dañarnos.

¿Qué es la criptografía?

Antes de comentar las aplicaciones que están funcionando en Internet, vamos a repasar brevemente qué es la criptografía. Se trata de un proceso que tiene dos partes. La primera es la encriptación o cifrado, que consiste en convertir cualquier tipo de información con cierto significado en un conjunto de símbolos o datos sin ningún sentido. La segunda parte del proceso criptográfico es el descifrado o desencriptación, que consiste en que el destinatario de dicha información pueda convertir los datos sin sentido en la información original. El cifrado consiste en una serie de algoritmos o funciones que permiten la conversión y posteriormente el descifrado. Estos algoritmos suelen basarse en una clave que tienen que tener en su poder tanto el que cifra el mensaje como el que lo descifra. Es decir, el emisor cifra el mensaje con un algoritmo aplicando una clave y el receptor lo descifra utilizando otro algoritmo y la misma *password*. Este sistema se denomina de clave simétrica o clave privada. Es el que históricamente se ha utilizado en aplicaciones, por ejemplo, de espionaje o inteligencia militar.

En la actualidad se utilizan algoritmos que funcionan con dos contraseñas distintas. Es decir, que el emisor no posee la misma clave que el receptor, pero cada *password* identifica a cada uno de ellos. La razón es que en redes como Internet, con millones de usuarios, si para cada comunicación entre dos usuarios hay que crear una clave, el número de ellas sería exorbitante (el cuadrado del número de usuarios de la Red, suponiendo que todos se comunican entre sí). Estos sistemas se denominan de clave pública y funcionan de la

siguiente manera. Cada usuario dispone de una contraseña privada y de una clave pública que lo identifica y que puede distribuir. Cualquiera puede utilizar la *password* pública de un usuario para cifrar un mensaje, mientras que el receptor utiliza entonces su clave privada para descifrarlo. Es decir, que la contraseña pública de un usuario sólo sirve para cifrar mensajes, pero no para descifrar mensajes para un usuario concreto. La firma digital funciona de forma inversa. Se utiliza una *password* privada para firmar documentos (una que sólo puede utilizar un usuario en concreto) y en cambio se aplica la clave pública para comprobar que efectivamente el documento ha sido firmado por ese usuario. Si antes decíamos que la criptografía ha supuesto uno de los avances más importantes para Internet, el sistema de clave pública o de clave asimétrica es, dentro la criptografía, el sistema que ha posibilitado las comunicaciones seguras por la Red.



Gracias a los protocolos de seguridad, en Internet es posible establecer transacciones electrónicas como la compra *on-line* sin peligro de que alguien pueda interceptar nuestros datos de pago y realizar compras a nuestra costa.

Existen pasarelas de pago, como PayPal, que se ocupan de que las transacciones económicas que se producen al utilizar el comercio electrónico estén controladas y protegidas, pero a la vez que sean muy sencillas de realizar.

SSL y TLS, transporte seguro

Dentro de Internet hay muchas ocasiones en las que precisamos que la comunicación sea segura. Por ejemplo cuando estamos rellenando un formulario en una página web con datos personales, cuando establecemos una comunicación por chat o mensajería instantánea o tuando enviamos un correo electrónico. En todos estos casos necesitamos, por un lado, que nuestra comunicación no corra el peligro de ser interceptada y, por otro, asegurarnos de que el usuario u organismo con el que estamos conectados (por ejemplo, si rellenamos un formulario en una web de un Ministerio) es realmente quien pensamos. Para conseguir este intercambio seguro de datos e identificación de entidades se ha desarrollado un sistema llamado TLS *(Transport Layer Security)* desarrollado a partir de su predecesor, el SSL (*Secure Sockets Layer*). Se trata de sistemas que funcionan como una capa sobre el protocolo de comunicaciones que utiliza la criptografía para asegurarse de que nadie intercepta las comunicaciones. A la vez, estos sistemas se aseguran de que el usuario está conectado a un servidor seguro. Para conseguirlo se emiten los certificados correspondientes; cada servidor seguro tiene uno emitido por una entidad certificadora de confianza que se ocupa de comprobar que la empresa o institución es quien dice ser. De esta forma se evita la suplantación de empresas o instituciones como bancos u organismos públicos a la hora de utilizar sus servicios *on-line*. Estas certificaciones tienen una caducidad y están sujetas a revisiones para no correr riesgos.

Desde nuestro navegador podemos examinar los certificados que se van cargando en nuestro ordenador enviado por parte de las empresas y organismos a los que accedemos a través de páginas web seguras utilizando protocolos como el SSL o el TLS.

Emisión de certificados

Su emisión depende de entidades certificadoras que en algunos casos son organismos estatales. También existen certificados de usuario que permiten a los propietarios de ciertas páginas (bancos,

Rastreadores de agujeros de seguridad

Si hablamos de cómo proteger la seguridad de las comunicaciones en Internet tenemos que referirnos inevitablemente a aquellos contra los que las protegemos. Popularmente se conoce como **hacker** a aquella persona con conocimientos de informática que trata de encontrar brechas en programas y redes informáticas para penetrar en sistemas protegidos. Por su parte, los **cracker** dan un paso más ya que utilizan ese acceso para obtener datos confidenciales, en la mayoría de los casos con fines lucrativos. Las «hazañas» de estos sujetos incluyen desde apropiarse de listados de datos sobre tarjetas de crédito hasta introducirse en ordenadores de organismos estatales para vender secretos a potencias extranjeras. En algunas ocasiones, el término *hacker* se ha utilizado, en general, para designar tanto a los que buscan agujeros de seguridad por afición o profesión como a los que los utilizan para sacar provecho. Sin embargo, hay que decir que los *hackers* han contribuido decisivamente a aumentar la seguridad de los sistemas y las comunicaciones al poner en evidencia los fallos de seguridad. Incluso se organizan competiciones con premios en metálico por parte de las empresas de seguridad para probar la inviolabilidad de sus productos y, de paso, darse publicidad. Existen incluso verdaderas olimpiadas de *hackers*, como la organizada en la conferencia **Defcon para hackers** en Las Vegas.

entidades públicas...) saber qué usuario se está conectando. Se trata de pequeños ficheros que almacenamos en nuestro ordenador. Para que el certificado sea efectivo, tendremos que configurar nuestro navegador para que lo utilice. De esta forma podemos acceder a ciertos servicios estando perfectamente identificados, ya que funcionan como clave pública para la transacción segura de datos..Tal y como vimos en el capítulo de protección de ordenadores, el DNI digital está sustituyendo en algunos casos a estos certificados electrónicos. En nuestro país existen varias entidades certificadoras públicas y privadas cuya lista puede consultarse en la web del Ministerio de Industria, Turismo y Comercio (www.mityc.es/DGDSI/Servicios/FirmaElectronica/Prestadores/). Así pues, una vez certificado el usuario y el proveedor del servicio, y una vez codificada la comunicación con las claves correspondientes, la transacción puede considerarse segura. Cuando se combina el protocolo HTTP (el de las páginas web) con sistemas como el TLS o el SSL, el protocolo pasa a denominarse HTTPS (agregando la S de seguridad). Cuando accedemos a una página segura, aparecerá el símbolo del candado en la parte inferior derecha del navegador. Eso sí, hay que aclarar que la aparición de este icono

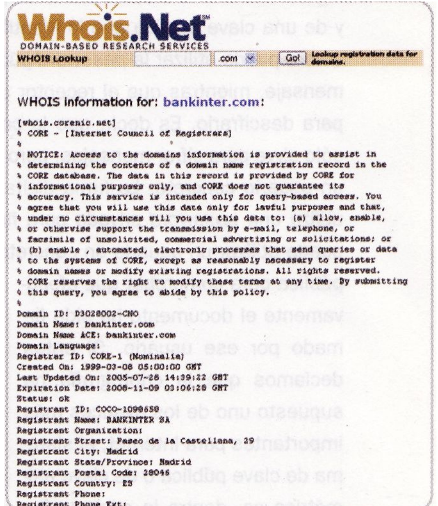


Si queremos acceder a ciertos servicios, como paginas web de la Administración, nosotros también tendremos que conseguir nuestro certificado electrónico que nos identifique. Entidédes como Ceres, que depende de la Fábrica Nacional de Moneda y Timbre, pueden proporcionarlo. Hay que tener en cuenta que los certificados caducan al cabo de un tiempo.

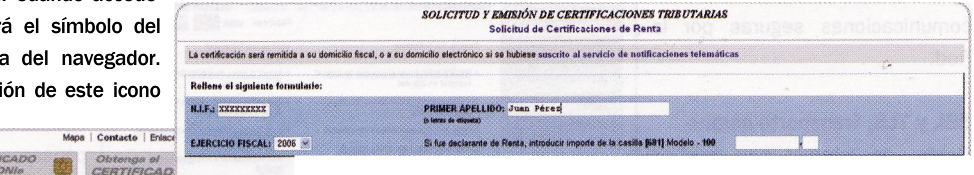
no garantiza la seguridad a menos que los certificados de seguridad y el protocolo funcionen perfectamente. En cualquier caso, no hay que proporcionar ninguna información confidencial (bancaria, personal...) a menos que veamos aparecer el candado.

Comercio electrónico seguro

Como hemos mencionado, uno de los procesos que más se ha visto beneficiado con la seguridad en las comunicaciones que proporcionan los procesos criptográficos es el comercio electrónico. Las pasarelas de intercambio seguro de datos como el TLS y el SSL permiten al usuario saber que está dando sus datos bancarios o tarjeta de crédito a una entidad de confianza que procederá a efectuar los trámites para el pago. Por otro lado, el comerciante se asegura de que la operación es válida a través de esta pasarela, sin tener más que encomendar la operación financiera a una entidad intermediaria y sin que los datos financieros o de la tarjeta del cliente lleguen a estar en ningún momento en su poder. Solamente tiene que entregar



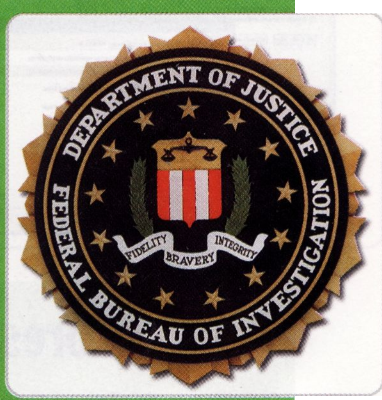
Si no estamos seguros de que la empresa de la página web a la que vamos a acceder es de confianza o corresponde a lo que creemos, podemos acceder al listado de WhoIs. Con sólo introducirla dirección web aparecerá el nombre de la empresa o institución además de otros datos.



Una vez certificados como usuarios podremos acceder a servicios de la Administración como la presentación telemática de declaraciones de Hacienda o la solicitud de certificados y documentos sin tener que movernos de casa.

¿Alguien lee nuestros mails?

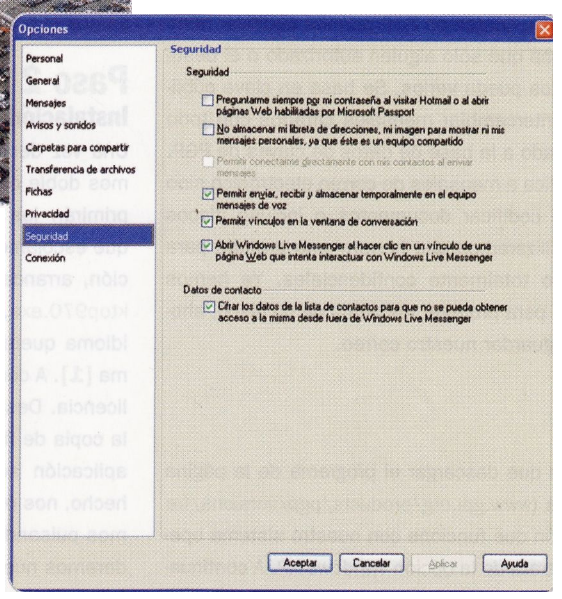
En realidad, nadie se dedica a leer todos los correos electrónicos que se intercambian los usuarios de Internet, pero sí es cierto que existen potentes sistemas capaces de detectar automáticamente si el contenido de los mensajes es, supuestamente, peligroso o atente contra la seguridad nacional. Los dos principales sistemas que monitorizan las comunicaciones son el Carnivore, que depende del FBI, y el Echelon, que depende de la NSA (la Agencia de Seguridad Nacional de Estados Unidos) y que recibe la colaboración de países como Nueva Zelanda, Australia, Japón o el Reino Unido. Estos sistemas interceptan las comunicaciones en grandes enlaces de comunicación (en el caso del primero en proveedores de Internet de EEUU, mientras que el Echelon lo hace en grandes nodos de fibra óptica alojados en los países colaboradores) y analizan los contenidos de los correos electrónicos para buscar palabras o términos que pudieran considerarse sensibles, como palabras relacionadas con terrorismo. Como muchos utilizamos servidores alojados en otros países, es posible que nuestras comunicaciones puedan ser interceptadas por esos sistemas, además de por *hackers* más tradicionales. No se conoce demasiado de estos sistemas de rastreo pero algunas asociaciones que se ocupan de seguridad han recomendado sistemas de criptografía para el correo electrónico para preservar la privacidad de los mensajes.



el producto a la dirección indicada y recibir el pago. Los métodos de pago seguros son varios, aunque los más populares son las pasarelas de entidades bancarias que permiten el cobro a través de tarjetas de crédito; aunque también hay otros métodos como el famoso PayPai o el envío de SMS (éste último para pequeñas cantidades de dinero) que también tienen su parque de usuarios.

Gracias a iniciativas como el OpenPGP podemos cifrar el contenido de nuestros mensajes de correo electrónico de forma que sólo el destinatario del mensaje pueda descifrarlo correctamente. Además, se trata de una herramienta gratuita.

La Agencia Nacional de Seguridad de los EEUU dispone de sistemas electrónicos, como el Echelon, para comprobar los contenidos de los correos electrónicos y otras transacciones que se producen por la red.



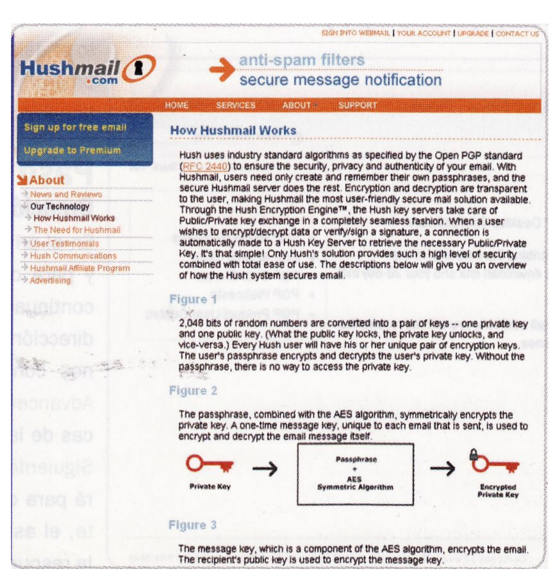
También en programas como el Messenger de Microsoft es posible preservar la privacidad de nuestras comunicaciones al activar las herramientas que el programa proporciona al respecto.

Como hemos visto, además de identificar a los intervinientes en la operación, los sistemas criptográficos aseguran que nadie pueda interceptar la información que se está intercambiando. De esta forma no corremos el peligro de que otra persona utilice los datos de dicha transacción para realizar compras *on-line* a nuestra costa. El problema de los pagos mediante tarjetas de crédito por Internet es que sólo se precisan los datos de la tarjeta, por lo que si la extraviamos o nos la roban es posible que alguien pueda utilizarla para comprar a nuestra costa. Para evitar este problema algunas pasarelas utilizan la dirección del titular de la tarjeta como comprobación. En cualquier 3aso, se puede decir que, salvo despiste, los métodos de protección de las transacciones de comercio electrónico son seguras.

Encriptación del correo

El correo, tanto el electrónico como el de papel, es quizás una de las formas de comunicación más personal que existe. En un *e-mail* o en una carta podemos enviar información confidencial, o simplemente ciertos contenidos que no nos gustaría que viesen otras personas. A pesar de que las comunicaciones dentro de Internet pueden establecerse de forma segura, en el caso del correo electrónico la seguridad es algo más débil. Los servidores de correo están en manos de entidades privadas y los *hackers* consiguen, en ocasiones, colarse en estos sistemas. Es decir, que ya no se está seguro simplemente sabiendo que la comunicación entre nuestro ordenador y el servidor correspondiente es segura, sino que también dependemos de la seguridad del propio servidor y de que la transmisión al destinatario también lo sea. Eso sin contar que en ciertos países, como EEUU, algunos organismos gubernamentales utilizan sistemas para comprobar que el contenido de los correos electrónicos sea correcto.

Pero existe una manera de asegurarse con casi total confianza de que un mensaje llegue solamente al destinatario del mismo: la criptografía aplicada al correo electrónico. En realidad se trata de volver a los orígenes del uso de la criptografía, en los que se utilizaban máquinas o algoritmos matemáticos para que, si era interceptado, un mensaje no pudiera ser descifrado por nadie que no fuera su destinatario. Para conseguir la absoluta confidencialidad de los mensajes, los sistemas de criptografía de correo electrónico funcionan con sistemas de clave pública, de los que ya hemos hablado. De esta manera sólo el destinatario real podrá leer correctamente el mensaje, sin necesidad de que sepamos su clave privada. Existen varios sistemas de criptografía para correo electrónico pero quizás el más popular es el PGP (en sus varias formas) o el S/MIME.



Existen servidores de correo web, como HusMail, que proporcionan un sistema de cifrado de mensajes mediante algoritmos como el PGP para proteger el contenido de nuestros correos electrónicos.

Que nadie lea tus correos

Utilizamos el sistema de clave pública PGP para cifrar nuestros mensajes

Es conveniente disponer de un sistema criptográfico que oculte los mensajes de correo electrónico que enviamos por la Red para asegurarnos de que sólo sus destinatarios pueden acceder a su contenido. Para conseguirlo, utilizaremos una herramienta basada en el sistema PGP.

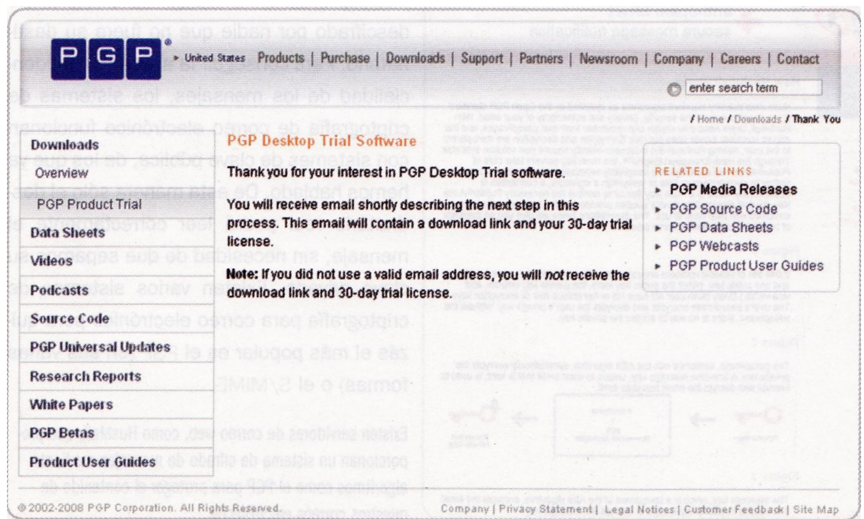
Antes de empezar, hay que tener en cuenta que, para que funcione, el destinatario también tendrá que tener instalado el programa y haber dado de alta la clave pública PGP correspondiente para que sea posible el intercambio de mensajes confidenciales.

El sistema de protección de contenido PGP permite codificar mensajes y documentos de forma que sólo alguien autorizado o el destinatario de estos documentos pueda verlos. Se basa en clave pública, por lo que podremos intercambiar mensajes cifrados con todo aquel que se haya incorporado a la base de datos de claves de PGP. Este sistema no sólo se aplica a mensajes de correo electrónico sino que también es capaz de codificar documentos o incluso discos duros. En nuestro caso, utilizaremos una herramienta gratuita para enviar mensajes de correo totalmente confidenciales. Ya hemos echado mano del programa para proteger los datos de un disco, ahora, lo usaremos para salvaguardar nuestro correo.

Paso 1

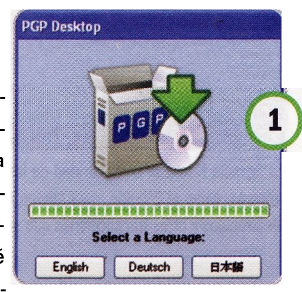
Descarga

En primer lugar, tendremos que descargar el programa de la página web de sus desabolladores (www.gp¡.org/products/pgp/versions/freeware) y elegir la distribución que funcione con nuestro sistema operativo; en nuestro caso, se trata de la opción Windows XP. A continuación, escogeremos PGP 8.0 y seguidamente la versión en inglés. Se presentará entonces la página de la empresa PGP Corporation. De entre los enlaces que encontraremos, elegiremos PGP Desktop 30-Day Free Tria!. A continuación, haremos clic en el enlace PGP Desktop Tria! Software (Desktop Client Only). En la página de información que le acompaña, se comenta que, aunque se trata de una versión de evaluación de 30 días, las funciones básicas seguirán funcionando tras el período de prueba, es decir, podremos desencriptar mensajes y encriptarlos manualmente. A continuación, pincharemos en el enlace ! have read and agree to the above EULA and Consent Notice, que se encuentra al pié de la página y rellenaremos el formulario con nuestra información de contacto. Cuando terminemos, nos enviará a la dirección de correo electrónico proporcionada un enlace para descargarnos el programa. Sólo nos restará hacer clic en Download.



Paso 2

Instalación

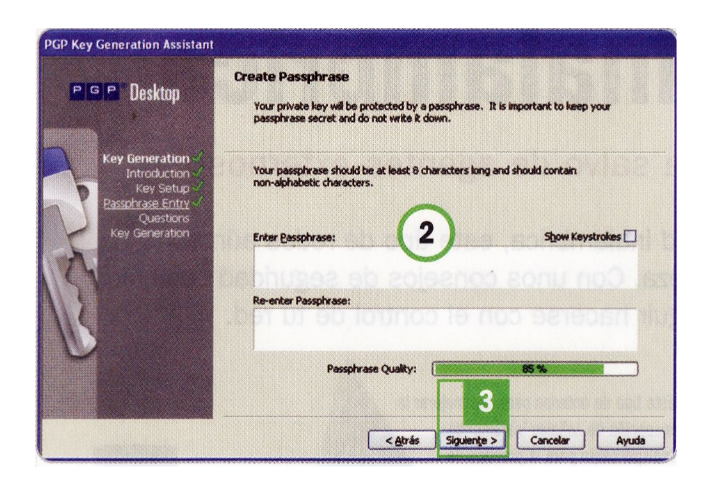


Una vez descargado el fichero, haremos doble clic sobre él y se descomprimirán los archivos en la carpeta que escojamos. Para iniciar la instalación, arrancamos el fichero PGPDesktop970.exe, que nos pedirá en qué idioma queremos emplazar el programa [1]. A continuación, tendremos que leer y aceptar el contrato de licencia. Después de aceptar los términos del contrato, comenzará la copia de ficheros. Finalmente, hemos de reiniciar el sistema y la aplicación se ejecutará para terminar con el proceso. Una vez hecho, nos preguntará si queremos activar el programa. Contestaremos pulsando en Yes y haciendo clic en Siguiente. A continuación, daremos nuestros datos para la licencia y pulsaremos de nuevo en Siguiente y nos pedirá el número de licencia (que podemos elegir descargarla para una prueba de 30 días). En nuestro caso, utilizaremos el software sin alguna de sus funciones, por lo que haremos clic en Use without iicence an disable most functionality. Al pulsar en Siguiente, nos mostrarán los módulos que van a funcionar. A continuación, nos indicará si queremos crear una nueva clave PGP. Si no disponemos de una, haremos clic en Yes y, luego, en Siguiente. Si nos saltamos ese paso, podremos acceder en cualquier momento al asistente de creación de claves dentro del programa haciendo clic en el menú File y, a continuación, en New pgp key.

Paso 3

Creación de la clave

En el primer paso, se expone qué es una clave y para qué sirve. Pulsaremos en Siguiente. A continuación, proporcionaremos el nombre y la dirección de correo electrónico para identificarnos con otras personas. Si nos dirigimos a Advanced, modificaremos algunas características de la clave. Para continuar, haremos clic en Siguiente e introduciremos una frase que servirá para codificarla [2]. Al hacer clic en Siguiente, el asistente nos pedirá que proporcionemos la respuesta a cinco preguntas personales por si

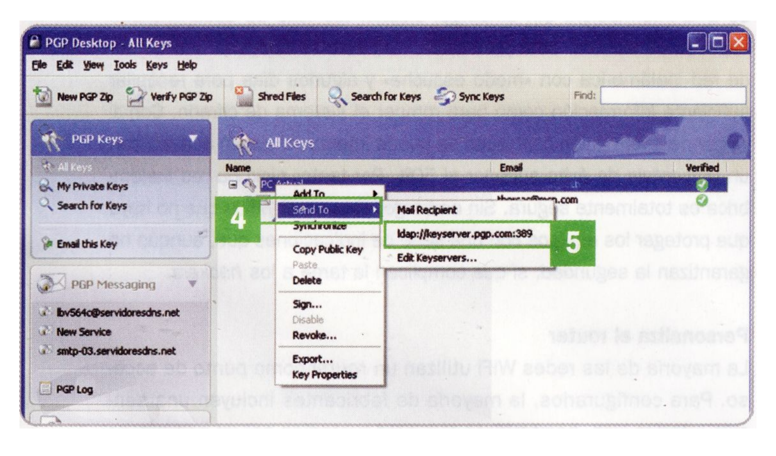


necesitamos recuperarla y no recordamos la frase. Finalmente se creará la clave, sólo tenemos que finalizar el proceso pulsando en Siguiente [3] y en Done. Automáticamente veremos cómo la clave se añade a nuestra base de datos de claves del programa.

Paso 4

Guarda y comparte la clave

Lo primero que haremos tras generar la clave es guardar una copla. De esta forma, podremos recuperarla o utilizarla con otro programa que se base en el mismo sistema de encriptación. Para ello, haremos doble clic en el icono del candado de la barra de tareas situado abajo a la derecha. Veremos que, en pantalla, aparece una lista con nuestra clave. A continuación, haremos clic en ella y abriremos el menú File, eligiendo la opción Export y, dentro de la misma, Key. Nos pedirá dónde queremos almacenar la clave y escogeremos el lugar en el disco que nos parezca oportuno. El siguiente paso consiste en com-

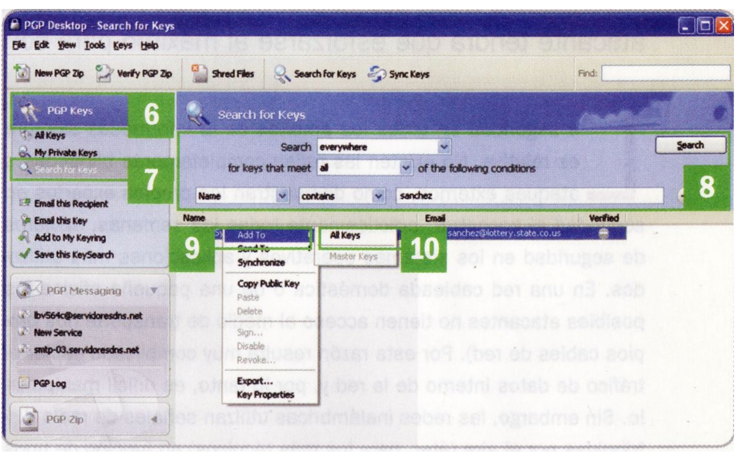


partir nuestra clave pública con un directorio, para que otros usuarios puedan mandarnos mensajes cifrados. Hay que recordar que esa clave sólo sirve para descifrar mensajes, por lo que no corremos ningún peligro al ponerla en común. Para hacerlo, haremos clic en la misma pulsando el botón derecho del ratón y elegiremos la opción Send to [4] y, dentro de ella, el servidor de claves, en este caso ldap://keyserver.pgp.com [5]. Como podemos ver, también es posible enviarla por correo electrónico, de esta manera proporcionará al contacto que queramos una clave para que pueda remitirnos mensajes cifrados.

Paso 5

Otros usuarios

El programa PGP Desktop se iniciará y aparecerá un icono de un candado en la barra de herramientas. Si hemos creado las claves, también veremos unas llaves. Para enviar un mensaje de correo electrónico, tendremos que comprobar que el destinatario de nuestro mensaje también tiene clave PGP. Para codificar el mensaje correctamente, necesitaremos tenerla, es decir, un fichero que la contenga. Para conseguirla, o bien nos la envía por correo electrónico o tendremos que buscarla en el servidor de claves. Para hacerlo, nos fijaremos en la parte de la ventana del programa llamada PGP Keys [6]. Dentro de ella, haremos clic en la zona denominada Search for Keys [7J. Apare-

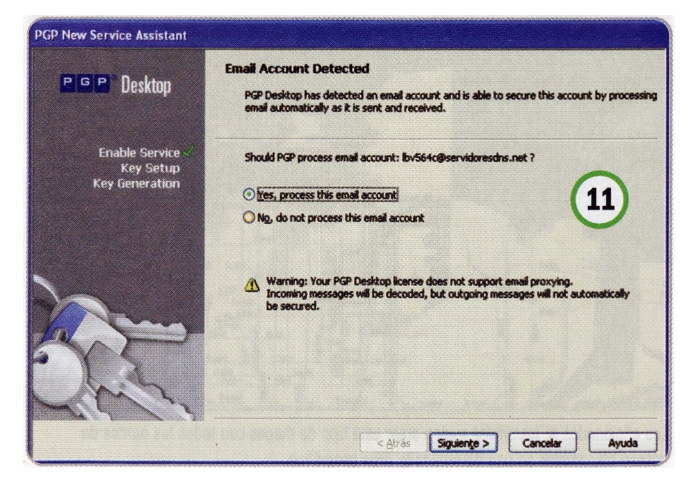


cerá un buscador [8] con el que podremos comprobar si nuestro contacto tiene clave pública almacenada en el servidor. Una vez encontrado al usuario, haremos clic con el botón derecho del ratón sobre su clave y elegiremos la opción Add To [9] y dentro de ella en All Keys [10]. Si volvemos a la lista de claves, veremos que se ha añadido.

Paso 6

Mensajes cifrados

Ya tenemos nuestra clave y vamos a enviar un mensaje cifrado. Simplemente, abriremos el cliente de correo y escribiremos un mensaje a un destinatario del que dispongamos su clave pública. Si le escribimos un *e-mail,* al enviarlo, el programa PGP lo detectará y añadirá ese servidor de correo a su base de datos. Si tenemos habilitados los protocolos de seguridad TLS o SSL con nuestro servidor de correo, el programa nos avisará que tenemos que desactivarlos, pues es el PGP quien se ocupará de ese cifrado. Una vez configurado el programa de correo, enviaremos de nuevo el mensaje. Entonces, aparecerá en pantalla una ventana que nos pedirá detalles sobre la clave que queremos utilizar para enviarlo [11]. Si la dirección de correo electrónico del destinatario está dentro de nuestro archivo de claves, el programa encriptará el mensaje de forma que sólo el destinatario pueda leerlo.



Protege tu red inalámbrica

Cómo mantener nuestra red doméstica a salvo de agentes externos

Aunque se han realizado grandes avances en seguridad inalámbrica, este tipo de redes aún son susceptibles a los ataques debido a su propia naturaleza. Con unos consejos de seguridad cualquier atacante tendrá que esforzarse al máximo para conseguir hacerse con el control de tu red.

La seguridad en todos los ámbitos de la informática siempre es relativa. No existen las redes completamente blindadas a ataques externos, como demuestran los propios expertos en seguridad al encontrar, prácticamente todas las semanas, agujeros de seguridad en los sistemas operativos y aplicaciones más utilizados. En una red cableada doméstica o de una pequeña oficina los posibles atacantes no tienen acceso al medio de transporte (los propios cables de red). Por esta razón resulta muy complicado espiar el tráfico de datos interno de la red y, por lo tanto, es difícil manipularlo. Sin embargo, las redes inalámbricas utilizan señales de radio distribuidas por el aire (éter, para los más técnicos) en función de unos patrones de emisión que no son fáciles de controlar. Por lo tanto, para un atacante es mucho más fácil interceptar las comunicaciones siempre que se encuentre dentro del radio de alcance del emisor *wireless*. Recordad que las señales de radio pueden atravesar paredes y alcanzar la calle o edificios cercanos.

Así, se han extendido prácticas como el *wardriving* en las calles de muchas ciudades. Ésta consiste en buscar señales *wireless* con un portátil o PDA desde un vehículo en movimiento. Muchos incluso utilizan dispositivos GPS para fijar la localización de las redes y registran sus hallazgos en sitos web como WiGLE (www.wigle.net). Estos datos pueden ser utilizados para acceder a redes sin protección.

Los aficionados al *wardriving* suelen crear este tipo de mapas con todos los puntos de acceso disponibles en una determinada área geográfica.

Este tipo de antenas permiten mejorar la recepción de señales inalámbricas. Indispensable para la práctica de *wardriving*.

Existe el convencimiento general de que las redes inalámbricas están actualmente bien protegidas gracias a funciones de seguridad como WEP de 128 bits o WPA. Éstas encriptan los datos emitidos en una red inalámbrica para que los «mirones» no tengan acceso a la información. Sin embargo, existen técnicas de desencriptado capaces de vulnerar esta protección. Tan sólo se necesita una tarjeta de red inalámbrica con «modo escucha» y algunos días para recopilar suficiente información como para romper el sistema de cifrado. Con 1 «giga» de información capturada se puede intentar el asalto a la red con un porcentaje de éxito superior al 50%. Por tanto, ninguna red inalámbrica es totalmente segura. Sin embargo, esto no significa que no haya que proteger los equipos con una serie de indicaciones que, aunque no garantizan la seguridad, sí que complican la tarea a los *hackers*.

Personaliza el router

La mayoría de las redes WiFi utilizan un *router* como punto de acceso. Para configurarlos, la mayoría de fabricantes incluyen una sencilla interfaz web, herramienta que está protegida por un nombre de usuario y una *password*. Todos los modelos iguales tienen, por defecto, los mismos datos de acceso y además éstos normalmente se publican en la propia web del fabricante o en *sites* especializados en seguridad. Por tanto, un atacante avispado podría acceder al *router* y cambiar la configuración del mismo con relativa facilidad.

Para dotar a un ordenador de una conexión *wireless* de calidad se puede recurrir a estas tarjetas PCI.

Desconfía de los puntos de acceso abiertos

Aunque resulten tremendamente útiles en algunas ocasiones, los puntos de acceso gratuitos (*hotspots*) situados en edificios de uso público como aeropuertos, restaurantes u hoteles, pueden ser más peligrosos de lo que cabría esperar. Estas redes están configuradas para facilitar la conexión de todo tipo de usuarios y dispositivos. Por esta razón, el nivel de seguridad suele ser mínimo. Por lo tanto, pueden convertirse en un foco de infección de especial virulencia e incluso ser el lugar ideal para robar información personal a otros usuarios. Por ejemplo, un usuario con una PDA basada en Windows y sin grandes conocimientos de tecnología de redes podría obtener información personal de prácticamente cualquier usuario conectado a una red sin seguridad. Así, en la red gratuita de un aeropuerto el mismo usuario sería capaz de conseguir cientos de claves (incluidas las corporativas) en apenas unos minutos. La solución, si se utilizan este tipo de puntos de conexión con relativa frecuencia, es protegerse con un buen *firewall* basado en software y una aplicación de protección de la información personal.



En un lugar público hay que extremar las precauciones antes de utilizar la conexión inalámbrica.



Cada vez más dispositivos utilizan conexiones inalámbricas; este equipo de música puede conectarse directamente a un punto de acceso.

Para evitar este riesgo, el primer paso que hay que dar al instalar este tipo de puntos de acceso es personalizar el nombre de usuario y la contraseña. Ésta es la única manera de que sólo el administrador de la red pueda modificar la configuración inalámbrica. Del mismo modo, el nombre de la red (denominado técnicamente SSID) también suele ser común en todos los dispositivos del mismo modelo. Sólo se necesita este nombre para conseguir la clave y el nombre de usuario por defecto del dispositivo desde la web del fabricante. Por lo tanto, también es imprescindible cambiar el SSID del punto de acceso o *router* durante la primera configuración del dispositivo.

Configura la seguridad

Los puntos de acceso o *routers* inalámbricos suelen emitir el nombre de la red (SSID) en intervalos regulares. Esta característica fue diseñada para facilitar la conexión de todo tipo de dispositivos, sobre todo en lugares públicos. Sin embargo, en una instalación doméstica o una pequeña oficina no es necesario ya que todos los usuarios de la red conocen el nombre de la misma y los datos de conexión. Así, si una red no se puede detectar significa que difícilmente podrá ser atacada, por lo que desactivar la emisión del SSID aumenta notablemente la seguridad de cualquier red inalámbrica.

Pero la principal medida de protección es activar el cifrado. Todos los equipos WiFi soportan algún tipo de cifrado de datos capaz de ocultar la información transmitida. Antes de elegir el tipo de cifrado que se va a utilizar es imprescindible informarse de la compatibilidad de los distintos elementos WiFi que se van a utilizar. Después, sólo falta seleccionar siempre el de mayor seguridad de todos (habitualmente WAP) con la clave de mayor longitud posible (128 o 256 bits). Esta protección no es invulnerable, pero para un atacante resultará poco rentable dedicar días a atacar una pequeña red local sin demasiada información relevante que sustraer.

Por último, la mayoría de *router* inalámbricos disponen de un filtro de direcciones MAC para aumentar la seguridad de la red. Cada dispositivo de red dispone una dirección MAC única e intransferible. Si se crea una lista con los elementos WiFi de la red, el propio *router* impedirá el acceso a la misma por parte de otros dispositivos (como un nuevo portátil o PDA). Así, sólo el administrador de la red decide qué dispositivos pueden utilizar esta conexión y, por tanto, la seguridad aumenta notablemente.





Cada vez más teléfonos móviles disponen de conexión WiFi sin necesidad de recurrir a dispositivos externos.

Direcciones IP seguras

La mayoría de las redes domesticas utilizan la asignación de direcciones dinámicas (DHCP). Esta tecnología es muy fácil de configurar; sin embargo, proporciona una ventaja a los *hackers* ya que pueden obtener una IP válida con tan sólo conectarse a la red. Por lo tanto, es muy recomendable desactivar el DHCP del *router* o punto de acceso y crear, de manera manual, una lista con las direcciones IP asignadas a cada uno de los dispositivos de la red local. Para conseguir protección extra es recomendable que el rango de direcciones IP utilizadas sea distinto al empleado por defecto. Por ejemplo, un rango como 10.0.0.x oculta a los ordenadores con mayor eficacia de posibles ataques realizados desde Internet.



El futuro de las comunicaciones inalámbricas

Desde que a finales de 2003 se lanzaran al mercado los primeros *routers* inalámbricos compatibles con el estándar 802.11g, un grupo de trabajo especial designado por IEEE ha trabajado para lanzar la nueva versión del estándar inalámbrico utilizado mundialmente, el 802.11n. En noviembre del pasado año se presentó el borrador 3.0 de esta nueva versión, por lo que se prevé su aprobación definitiva para junio de 2009. La fecha de lanzamiento oficial de productos que utilicen este estándar tendrá que retrasarse aun más, aunque ya hay fabricantes como Belkin que garantizan que algunos de sus productos, como el F5D8230-4 Pre-N, serán totalmente compatibles con este estándar. Dentro de las esperadas mejoras de 802.11n destaca una velocidad de transmisión que multiplica por cinco la capacidad del estándar anterior (hasta los 248 Mbit/seg) y prácticamente duplica el rango útil de estos dispositivos hasta los 70 metros en interior y 250 en exterior. Estas tasas de transmisión increíbles permitirán, entre otras aplicaciones, la difusión en tiempo real de películas en formato 1080p (alta definición).

Algunos dispositivos ya presumen de su compatibilidad con 802.11n incluso antes de que el estándar esté aprobado por IEEE.

Para mejorar la seguridad de los ordenadores conectados a la red inalámbrica también es recomendable activar el cortafuegos que casi todos los *routers* incluyen. Además es altamente recomendable la instalación de un *firewall* personal basado en software en cada equipo.

Entorno inalámbrico definido

Las señales WiFi normalmente alcanzan el exterior de los edificios. Si apenas supera unos metros los muros del recinto no supone un gran problema, pero cuanto más lejos alcance la señal, más sencillo será atacar la red. Por lo tanto, cuando se instala una red inalámbrica en una casa o una pequeña oficina hay que asegurarse de que el *router* está situado aproximadamente en el centro del recinto. Colocarlo cerca de las ventanas o en un extremo del edificio puede provocar que la señal se distribuya decenas de metros por el exterior. Algunos modelos de puntos de acceso también ofrecen la posibilidad de limitar la potencia de las señales. Asf, en un hogar pequeño, quizás no sea necesario emitir a la máxima potencia para conseguir una tasa de transmisión alta. Ajustar este parámetro puede ser la diferencia entre una red altamente expuesta y otra de difícil acceso.

Del mismo modo, durante los periodos de tiempo largos en los que no se va a utilizar el *router*, por ejemplo en vacaciones, es muy recomendable apagarlo. Así, obviamente, será imposible atacar la red. Del mismo modo, hay que apagar el resto de dispositivos de la red como conexiones inalámbricas de portátiles, tarjetas WiFi... En el caso de estos últimos dispositivos hay que recordar que, aunque no se esté transmitiendo información, si el dispositivo de acceso está encendido el equipo que lo está utilizando continúa buscando nuevas redes y emitiendo paquetes de información de control, por lo que puede ralentizar el equipo y «estresar» a sus componentes.

Amenazas a través de Bluetooth

Aunque la mayoría de los usuarios sólo utilizan esta tecnología inalámbrica para conectar dispositivos como auriculares o teléfonos móviles, también se pueden utilizar para crear redes de ordenadores de carácter temporal. Por ejemplo, dos usuarios con portátiles pueden utilizar esta conexión para transmitirse archivos de manera sencilla. El problema es que este tipo de conexiones suelen ser punto a punto; es decir, la comunicación es directa y no interviene ningún elemento de seguridad intermedio. Además, el alcance de un dispositivo Bluetooth de clase 1 puede llegar a los 100 metros, por lo que en algunos lugares como un aeropuerto supone que miles de personas podrían tener acceso a la comunicación. Por si esto fuera poco, los dispositivos Bluetooth también son susceptibles de ataques basados en denegación de servicio (DoS).

Los usuarios de la plataforma Mac ya están habituados al funcionamiento de su punto de acceso Airport.

Por todo ello, para asegurar este tipo de conexiones es necesario asegurarse de que los dispositivo tienen activado algún tipo de seguridad. El Modelo 2 proporciona seguridad a nivel de servicio después de que se crea la conexión, mientras que el Modelo 3 proporciona seguridad a nivel del enlace; es decir, antes incluso de que se cree la conexión. En ambos casos, cuando dos dispositivos Bluetooth establecen una conexión ambos crean una clave de inicialización. Ésta se utiliza para encriptar la comunicación por lo que cuanto más larga sea esta clave, más difícil será romper el sistema de seguridad. Además, la contraseña debe ser cambiada con relativa frecuencia ya que un atacante podría recopilar los datos enviados con Bluetooth día tras día hasta tener suficiente información para vulnerar el sistema de seguridad.



Al orientar la antena de un punto de acceso inalámbrico se puede reducir el riesgo de seguridad y la potencia de las emisiones fuera de casa.





López de Hoyos, 141, 5º. 28002 Madrid (España)
Tel. 91 510 66 00. Fax 91 519 48 13